EUROOPA LIIT

EUROOPA PARLAMENT **NÕUKOGU**

Brüssel, 11. aprill 2024
(OR. en)

2021/0136(COD)
LEX 2318

PE-CONS 68/1/23
REV 1

TELECOM 351
COMPET 1163
MI 1028
DATAPROTECT 329
JAI 1550
CODEC 2237

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, MILLEGA MUUDETAKSE MÄÄRUST (EL) NR 910/2014 SEOSES EUROOPA DIGIIDENTITEEDI RAAMISTIKU KEHTESTAMISEGA

EUROOPA PARLAMENDI JA NÕUKOGU
MÄÄRUS (EL) 2024/…,

11. aprill 2024,

millega muudetakse määrust (EL) nr 910/2014 seoses
Euroopa digiidentiteedi raamistiku kehtestamisega

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[1],

võttes arvesse Regioonide Komitee arvamust[2],

toimides seadusandliku tavamenetluse kohaselt[3]

---

1 ELT C 105, 4.3.2022, lk 81.
2 ELT C 61, 4.2.2022, lk 42.
3 Euroopa Parlamendi 29. veebruari 2024. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 26. märtsi 2024. aasta otsus.

ning arvestades järgmist:

(1) Komisjoni 19. veebruari 2020. aasta teatises „Euroopa digituleviku kujundamine“ teatatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014[4] läbivaatamisest, et muuta selle toimimine tõhusamaks, laiendada selle positiivset mõju erasektorile ja edendada usaldusväärseid digiidentiteete kõigi eurooplaste jaoks.

(2) Euroopa Ülemkogu kutsus oma 1.–2. oktoobri 2020. aasta järeldustes komisjoni üles tegema ettepanekut töötada välja kogu liitu hõlmav turvalise avaliku elektroonilise identimise raamistik, sealhulgas koostalitlusvõimelised digiallkirjad, et anda inimestele kontroll oma internetiidentiteedi ja andmete üle ning võimaldada juurdepääsu avalikele, eraõiguslikele ja piiriülestele digiteenustele.

(3) Euroopa Parlamendi ja nõukogu otsusega (EL) 2022/2481[5] loodud digikümnendi poliitikaprogrammis 2030 on kindlaks määratud liidu raamistiku eesmärgid ja digisihid, mille eesmärk on 2030. aastaks viia usaldusväärse, vabatahtliku ja kasutaja kontrolli all oleva digiidentiteedi ulatusliku kasutuselevõtuni, mida tunnustatakse kogu liidus ja mis võimaldab igal kodanikul kontrollida enda andmeid internetitoimingute käigus.

---

[4] Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.8.2014, lk 73).

[5] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta otsus (EL) 2022/2481, millega luuakse digikümnendi poliitikaprogramm 2030 (ELT L 323, 19.12.2022, lk 4).

(4) Euroopa Parlamendi, nõukogu ja komisjoni välja kuulutatud „Euroopa deklaratsioonis digiõiguste ja -põhimõtete kohta digikümnendiks“[6] (edaspidi „deklaratsioon“) rõhutatakse igaühe õigust pääseda juurde digitehnoloogiale, -toodetele ja -teenustele, mis on sisseprojekteeritult ohutud, turvalised ja privaatsust kaitsvad. Muu hulgas tagatakse, et kõigile liidus elavatele inimestele pakutakse juurdepääsetavat, turvalist ja usaldusväärset digiidentiteeti, mis annab juurdepääsu mitmesugustele internetipõhistele ja võrguvälistele teenustele, mis on kaitstud kõigi küberriskide ja küberkuritegevuse, sealhulgas andmetega seotud rikkumiste ja identiteedivarguse või identiteediga manipuleerimise eest. Deklaratsioonis märgitakse ka, et igaühel on õigus sellele, et tema isikuandmed oleksid kaitstud. See õigus tähendab muu hulgas kontrolli selle üle, kuidas neid andmeid kasutatakse ja kellega neid jagatakse.

(5) Liidu kodanikel ja elanikel peaks olema õigus digiidentiteedile, mis on nende ainukontrolli all ja mis võimaldab neil kasutada oma õigusi digikeskkonnas ja osaleda digimajanduses. Selle eesmärgi saavutamiseks tuleks luua Euroopa digiidentiteedi raamistik, mis võimaldab liidu kodanikele ja elanikele juurdepääsu avalikele ja eraõiguslikele internetipõhistele ja võrguvälistele teenustele kogu liidus.

(6) Ühtlustatud digiidentiteedi raamistik peaks aitama luua digitaalsemalt integreeritud liitu, vähendades liikmesriikidevahelisi digitõkkeid ning andes liidu kodanikele ja elanikele võimaluse kasutada digitaliseerimise eeliseid, suurendades samal ajal läbipaistvust ja nende õiguste kaitset.

---

[6] ELT C 23, 23.1.2023, lk 1.

(7) Ühtsem e-identimise käsitus peaks vähendama riske ja kulusid, mille põhjus on praegune erinevate riiklike lahenduste kasutamisest tulenev killustatus või mõnes liikmesriigis selliste e-identimise lahenduste puudumine. Selline käsitus peaks tugevdama siseturgu, võimaldades liidu kodanikel, liidu elanikel, nagu on määratletud riigisiseses õiguses, ja ettevõtjatel end kogu liidus internetis ja väljaspool seda turvalisel, usaldusväärsel, kasutajasõbralikul, mugaval, ligipääsetaval ja ühtlustatud viisil identifitseerida ja oma identiteeti autentida. Euroopa digiidentiteedikukkur peaks andma füüsilistele ja juriidilistele isikutele kogu liidus ühtlustatud e-identimise vahendi, mis võimaldab neil oma identiteediga seotud andmeid autentida ja jagada. Igaühel peaks olema turvaline juurdepääs avalikele ja erasektori teenustele, tuginedes usaldusteenuste täiustatud ökosüsteemile ning kontrollitud isikut tõendavatele dokumentidele ja elektroonilistele tõenditele, nagu akadeemiline kvalifikatsioon, sealhulgas ülikoolikraadid või muud haridus- või kutsealased õigused. Euroopa digiidentiteedi raamistiku eesmärk on minna üksnes riiklikele digitaalse identiteedi lahendustele tuginemiselt üle kogu liidus kehtivate ja õiguslikult tunnustatud elektrooniliste tõendite esitamisele. Elektrooniliste tõendite pakkujate suhtes tuleks kohaldada selgeid ja ühtseid normistikke, samal ajal kui haldusasutused peaksid saama tugineda teatavas vormingus e-dokumentidele.

(8) Mitu liikmesriiki on rakendanud ja kasutavad e-identimise vahendeid, mida liidu teenuseosutajad aktsepteerivad. Lisaks on määruse (EL) nr 910/2014 alusel investeeritud nii riiklikesse kui ka piiriülestesse lahendustesse, sealhulgas teavitatud e-identimise süsteemide koostalitlusvõimesse vastavalt kõnealusele määrusele. Selleks et tagada Euroopa digiidentiteedikukrute vastastikune täiendavus ja kiire kasutuselevõtt teatatud e-identimise vahendite praeguste kasutajate poolt ning minimeerida mõju olemasolevatele teenuseosutajatele, peaksid Euroopa digiidentiteedikukrud oodatavalt toetuma kogemustele, mis on saadud seoses olemasolevate e-identimise vahendite ning liidu ja riiklikul tasandil kasutusele võetud teavitatud e-identimise süsteemide taristuga.

(9) Kõigi määruse (EL) nr 910/2014 kohaste isikuandmete töötlemise toimingute suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2016/679[7] ning vajaduse korral Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ[8]. Käesolevas määruses sätestatud koostalitlusvõime raamistiku lahendused järgivad samuti kõnealuseid norme. Liidu andmekaitseõiguses on sätestatud andmekaitse põhimõtted, nagu võimalikult väheste andmete kogumise ja eesmärgi piiritlemise põhimõte, ning kohustused, nagu lõimitud ja vaikimisi andmekaitse.

---

[7] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

[8] Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37).

(10) Liidu ettevõtjate konkurentsivõime toetamiseks peaks nii internetipõhiste kui veebiväliste teenuste osutajatel olema võimalik tugineda digiidentiteedi lahendustele, mida tunnustatakse kogu liidus, olenemata liikmesriigist, kus neid lahendusi osutatakse, ning saada seega kasu ühtlustatud liidu käsitusest usaldusele, turvalisusele ja koostalitlusvõimele. Nii kasutajatel kui ka teenuseosutajatel peaks olema kindlus, et elektroonilistel tõenditel on sama õigusjõud kogu liidus. Ühtlustatud digiidentiteedi raamistiku eesmärk on luua majanduslikku väärtust, võimaldades hõlpsamat juurdepääsu kaupadele ja teenustele ning vähendades märkimisväärselt e-identimise ja e-autentimise menetlustega seotud tegevuskulusid, näiteks uute klientide aktiveerimisel, vähendades selliste küberkuritegude nagu identiteedivargus, andmevargus ja internetipettus esinemisvõimalusi, edendades seeläbi tõhusust ning liidu mikro-, väikeste ja keskmise suurusega ettevõtjate (VKEd) turvalist digiüleminekut.

(11) Euroopa digiidentiteedikukrud peaksid hõlbustama andmete ühekordse küsimise põhimõtte kohaldamist, vähendades seeläbi liidu kodanike ja elanike ning ettevõtjate halduskoormust ja toetades nende piiriülest liikuvust kogu liidus ning edendades koostalitlusvõimeliste e-valitsuse teenuste arendamist kogu liidus.

(12) Käesoleva määruse rakendamisel toimuva isikuandmete töötlemise suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määrusi (EL) 2016/679 ja (EL) 2018/1725[9] ning direktiivi 2002/58/EÜ. Seepärast tuleks käesolevas määruses sätestada konkreetsed kaitsemeetmed, et e-identimise vahendite ja elektrooniliste tõendite pakkujad ei saaks kombineerida muude teenuste osutamisel saadud isikuandmeid käesoleva määruse kohaldamisalasse kuuluvate teenuste osutamise eesmärgil töödeldud isikuandmetega. Euroopa digiidentiteedikukrute pakkumisega seotud isikuandmeid tuleks hoida loogiliselt lahus kõigist muudest Euroopa digiidentiteedikukru pakkuja valduses olevatest andmetest. Käesolev määrus ei tohiks takistada Euroopa digiidentiteedikukrute pakkujatel kohaldamast täiendavaid tehnilisi meetmeid, mis aitavad kaitsta isikuandmeid, nagu Euroopa digiidentiteedikukrute pakkumisega seotud isikuandmete füüsiline eraldamine muudest pakkuja valduses olevatest andmetest. Ilma et see piiraks määruse (EL) 2016/679 kohaldamist, täpsustatakse käesolevas määruses eesmärgi piiritlemise, võimalikult väheste andmete kogumise ning lõimitud ja vaikimisi andmekaitse põhimõtete kohaldamist.

[9] Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

(13) Euroopa digiidentiteedikukrute üks integreeritud funktsioon peaks olema ühine töölaud, et tagada kasutajatele suurem läbipaistvus, privaatsus ja kontroll oma isikuandmete üle. Kõnealune funktsioon peaks pakkuma lihtsat ja kasutajasõbralikku liidest ülevaate saamiseks kõigist tuginevatest isikutest, kellega kasutaja andmeid jagab, sealhulgas atribuutidest, ja andmete liigist, mida iga tugineva isikuga jagatakse. See peaks võimaldama kasutajatel jälgida kõiki Euroopa digiidentiteedikukru kaudu tehtud tehinguid, hõlmates vähemalt järgmiseid andmeid: tehingu kellaaeg ja kuupäev, vastaspoole identiteet, taotletud isikuandmed ja jagatud andmed. Need andmed tuleks salvestada ka juhul, kui tehingut ei sõlmitud. Tehingu ajaloos sisalduva teabe autentsust ei tohiks olla võimalik kahtluse alla seada. Selline funktsioon peaks olema vaikimisi aktiivne. See peaks võimaldama kasutajatel lihtsalt taotleda tuginevalt isikult isikuandmete viivitamatut kustutamist vastavalt määruse (EL) 2016/679 artiklile 17 ja lihtsalt teatada tuginevast isikust pädevale riiklikule andmekaitseasutusele, kui Euroopa digiidentiteedikukru kaudu on otse saadud väidetavalt ebaseaduslik või kahtlane isikuandmete taotlus.

(14) Liikmesriigid peaksid integreerima Euroopa digiidentiteedikukrusse erinevad privaatsust säilitavad tehnoloogiad, näiteks teabetu tõestus. Need krüptomeetodid peaksid võimaldama tugineval isikul kontrollida, kas isikutuvastusandmetel ja atribuutide tõenditel põhinev kinnitus on tõene, avaldamata andmeid, millel see kinnitus põhineb, säilitades seeläbi kasutaja privaatsuse.

(15) Käesolevas määruses sätestatakse ühtlustatud tingimused liikmesriikide poolt kättesaadavaks tehtavate Euroopa digiidentiteedikukrute raamistiku loomiseks. Kõigil liidu kodanikel ja riigisiseses õiguses määratletud liidu elanikel peaks olema õigus turvaliselt taotleda, valida, kombineerida, salvestada, kustutada, jagada ja esitada oma identiteediga seotud andmeid ning taotleda oma isikuandmete kustutamist kasutajasõbralikul ja mugaval viisil kasutaja ainukontrolli all, võimaldades samal ajal isikuandmete valikulist avaldamist. Käesolev määrus kajastab ühiseid Euroopa väärtusi ja austab põhiõigusi, õiguslikke tagatisi ja vastutust, kaitstes seeläbi demokraatlikke ühiskondi, liidu kodanikke ja elanikke. Nende eesmärkide saavutamiseks kasutatava tehnoloogia väljatöötamisel tuleks sihiks seada kõrgeimal tasemel turvalisus, privaatsus, kasutajamugavus, juurdepääsetavus, lai kasutatavus ja sujuv koostalitlusvõime. Liikmesriigid peaksid tagama kõigile oma kodanikele ja elanikele võrdse juurdepääsu e-identimisele. Liikmesriigid ei tohiks otse ega kaudselt piirata nende füüsiliste või juriidiliste isikute juurdepääsu avalikele või erateenustele, kes ei otsusta kasutada Euroopa digiidentiteedikukruid, ning peaksid tegema kättesaadavaks asjakohased alternatiivsed lahendused.

(16) Liikmesriigid peaksid kasutama käesoleva määrusega pakutavaid võimalusi, et teha oma vastutusel Euroopa digiidentiteedikukruid kättesaadavaks nende territooriumil elavatele füüsilistele ja juriidilistele isikutele kasutamiseks. Selleks et pakkuda liikmesriikidele paindlikkust ja kasutada ära tipptasemel tehnoloogiat, peaks käesolev määrus võimaldama Euroopa digiidentiteedikukrute pakkumist otse liikmesriigi poolt, liikmesriigi volitusel või liikmesriigist sõltumatult, viimasel juhul peab liikmesriik selliselt pakutuid kukruid tunnustama.

(17) Registreerimiseks peaksid tuginevad isikud esitama teabe, mida on vaja nende e-identimiseks ja e-autentimiseks Euroopa digiidentiteedikukrute jaoks. Kui tuginevad isikud teatavad Euroopa digiidentiteedikukru kavandatavast kasutusest, peaksid nad esitama teabe andmete kohta, mida nad oma teenuste osutamiseks taotlevad, ja taotluse põhjuse. Tuginevate isikute registreerimine hõlbustab liikmesriikide poolset kontrolli tuginevate isikute tegevuse seaduslikkuse üle, mida tehakse kooskõlas liidu õigusega. Käesolevas määruses sätestatud registreerimiskohustus ei tohiks piirata muus liidu või riigisiseses õiguses sätestatud kohustuste täitmist, näiteks määruse (EL) 2016/679 kohaselt andmesubjektidele teabe esitamise kohustuse täitmist. Tuginevad isikud peaksid järgima kõnealuse määruse artiklites 35 ja 36 sätestatud kaitsemeetmeid, eelkõige tehes andmekaitsealaseid mõjuhinnanguid ja konsulteerides enne andmete töötlemist pädevate andmekaitseasutustega, kui andmekaitsealased mõjuhinnangud näitavad, et töötlemine tooks kaasa suure riski. Sellised kaitsemeetmed peaksid toetama isikuandmete seaduslikku töötlemist tuginevate isikute poolt, eelkõige andmete eriliikide, näiteks terviseandmete puhul. Tuginevate isikute registreerimise eesmärk on suurendada läbipaistvust ja usaldust Euroopa digiidentiteedikukrute kasutamise vastu. Registreerimine peaks olema kulutõhus ja seotud riskidega proportsionaalne, et tagada teenuse kasutuselevõtt teenuseosutajate poolt. Sellega seoses tuleks registreerimise käigus ette näha automatiseeritud menetluste kasutamine, sealhulgas olemasolevatele registritele tuginemine ja nende kasutamine liikmesriikide poolt, ning see ei tohiks hõlmata eelneva loa andmise menetlust. Registreerimisprotsess peaks võimaldama arvesse võtta erinevaid kasutusjuhte, mis võivad erineda registreerimisnõuete, tööreżiimi, s.t ka võrgus toimuv või võrguväline, või Euroopa digiidentiteedikukruga liidestamist võimaldavate seadmete autentimise nõude poolest. Registreerimist tuleks kohaldada üksnes selliste tuginevate isikute suhtes, kes osutavad teenuseid digitaalse suhtluse kaudu.

(18) Liidu kodanike ja elanike kaitsmine Euroopa digiidentiteedikukrute loata või petturliku kasutamise eest on väga oluline, et tagada usaldus Euroopa digiidentiteedikukrute vastu ja nende laialdane kasutuselevõtt. Kasutajatele tuleks tagada toimiv kaitse sellise väärkasutuse eest. Eelkõige juhul, kui liikmesriigi õigusasutus tuvastab muu menetluse raames asjaolud, mis on Euroopa digiidentiteedikukru petturliku või muul viisil ebaseadusliku kasutamise aluseks, peaksid Euroopa digiidentiteedikukru väljastajate eest vastutavad järelevalveasutused pärast teavitamist võtma vajalikud meetmed tagamaks, et tugineva isiku registreerimine ja tuginevate isikute lisamine autentimismehhanismi tunnistatakse kehtetuks või peatatakse seni, kuni teavitav asutus kinnitab, et tuvastatud rikkumised on kõrvaldatud.

(19) Kõik Euroopa digiidentiteedikukrud peaksid võimaldama kasutajatel end piiriüleselt elektrooniliselt identida ja autentida nii võrgus kui ka võrguväliselt, et pääseda juurde mitmesugustele avalikele ja erasektori teenustele. Ilma et see piiraks liikmesriikide eelisõigusi oma kodanike ja elanike identimisel, võivad Euroopa digiidentiteedikukrud täita ka haldusasutuste, rahvusvaheliste organisatsioonide ning liidu institutsioonide, organite ja asutuste institutsioonilisi vajadusi. Võrguväline autentimine oleks oluline paljudes sektorites, sealhulgas tervishoiusektoris, kus teenuseid osutatakse sageli inimesega vahetult suheldes, ning digiretseptide puhul peaks autentsuse kontrollimiseks olema võimalik tugineda ruutkoodile või sarnasele tehnoloogiale. E-identimise süsteemide kõrgele usaldusväärsuse tasemele tuginevad Euroopa digiidentiteedikukrud peaksid käesoleva määruse kohaste turvanõuete täitmiseks kasutama ära võltsimiskindlate lahenduste, näiteks turvaelementide potentsiaali. Euroopa digiidentiteedikukrud peaksid samuti võimaldama kasutajatel luua ja kasutada kogu liidus aktsepteeritavaid kvalifitseeritud e-allkirju ja e-templeid. Kui Euroopa digiidentiteedikukkur on aktiveeritud, peaks füüsilistel isikutel olema võimalik seda kasutada vaikimisi ja tasuta kvalifitseeritud e-allkirjaga allkirjastamiseks, ilma et nad peaksid läbima täiendavaid haldusmenetlusi. Kasutajad peaksid saama allkirjastada või tembeldada enda esitatud avaldusi või atribuute. Lihtsustamise eesmärgil ning inimeste ja ettevõtjate kulude vähendamiseks kogu liidus, sealhulgas võimaldades esindusõiguste ja e-volituse andmist, peaksid liikmesriigid pakkuma ühistele standarditele ja tehnilistele kirjeldustele tuginevaid Euroopa digiidentiteedikukruid, et tagada sujuv koostalitlusvõime ja parandada piisavalt IT-turvalisust, tugevdada vastupidavust küberrünnete vastu ning seega vähendada märkimisväärselt liidu kodanike ja elanike ning ettevõtjate võimalikke riske, mis tulenevad käimasolevast digiteerimisest.

Ainult liikmesriikide pädevad asutused saavad tagada usaldusväärsuse kõrge taseme isikusamasuse tuvastamisel ja anda seega kindluse, et ennast teatud isikuna esitlev isik on tõepoolest isik, kes ta väidab end olevat. Seepärast peaks Euroopa digiidentiteedikukrute pakkumine tuginema liidu kodanike, elanike või juriidiliste isikute õiguslikult määratletud identiteedile. Õiguslikult määratletud identiteedile tuginemine ei tohiks takistada Euroopa digiidentiteedikukru kasutajate juurdepääsu teenustele varjunime all, kui õiguslikult määratletud identiteedi autentimiseks puudub õiguslik nõue. Usaldust Euroopa digiidentiteedikukrute vastu suurendaks asjaolu, et neid väljastavad ja haldavad isikud peavad rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada kooskõlas määrusega (EL) 2016/679 turvalisuse kõrgeim tase, mis vastab füüsiliste isikute õigusi ja vabadusi ähvardavatele ohtudele.

(20) Kvalifitseeritud e-allkirja kasutamine muudel kui kutselistel eesmärkidel peaks olema kõigile füüsilistele isikutele tasuta. Liikmesriikidel peaks olema võimalik sätestada meetmed, mis takistavad füüsilistel isikutel kvalifitseeritud e-allkirjade tasuta kasutamist kutsealastel eesmärkidel, tagades samal ajal, et kõik sellised meetmed on tuvastatud riskidega proportsionaalsed ja põhjendatud.

(21) Kasulik on hõlbustada Euroopa digiidentiteedikukrute kasutuselevõttu ja kasutamist, integreerides need sujuvalt riiklikul, kohalikul või piirkondlikul tasandil juba kasutatavate avaliku ja erasektori digiteenuste ökosüsteemi. Selle eesmärgi saavutamiseks peaks liikmesriikidel olema võimalik sätestada õiguslikud ja korralduslikud meetmed, et suurendada paindlikkust Euroopa digiidentiteedikukrute pakkujate jaoks ja võimaldada Euroopa digiidentiteedikukrute lisafunktsioone lisaks käesolevas määruses sätestatule, sealhulgas suurendades koostalitlusvõimet olemasolevate riiklike e-identimise vahenditega. Sellised lisafunktsioonid ei tohiks mingil juhul kahjustada käesolevas määruses sätestatud Euroopa digiidentiteedikukrute põhifunktsioonide täitmist ega edendada Euroopa digiidentiteedikukrute asemel olemasolevaid riiklikke lahendusi. Kuna need lisafunktsioonid ulatuvad käesolevast määrusest kaugemale, ei kohaldata nende suhtes käesoleva määruse sätteid, mis käsitlevad piiriülest tuginemist Euroopa digiidentiteedikukrutele.

(22) Euroopa digiidentiteedikukrutel peaks olema funktsioon, millega luuakse kasutaja valitud ja hallatavaid varjunimesid, mida kasutatakse autentimiseks internetipõhistele teenustele juurdepääsul.

(23) Et saavutada turvalisuse ja usaldusväärsuse kõrge tase, kehtestatakse käesoleva määrusega Euroopa digiidentiteedikukrutele esitatavad nõuded. Euroopa digiidentiteedikukrute vastavust neile nõuetele peaksid sertifitseerima liikmesriikide määratud akrediteeritud vastavushindamisasutused.

(24) Selleks et vältida erinevaid käsitusi ja ühtlustada käesolevas määruses sätestatud nõuete rakendamist, peaks komisjon Euroopa digiidentiteedikukrute sertifitseerimiseks vastu võtma rakendusakte, et kehtestada võrdlusstandardite loetelu ning vajaduse korral kehtestada kirjeldused ja menetlused kõnealuste nõuete üksikasjalike tehniliste kirjelduste esitamiseks. Kui käesolevas määruses osutatud olemasolevad küberturvalisuse sertifitseerimise kavad ei hõlma Euroopa digiidentiteedikukrute vastavuse sertifitseerimist asjakohastele küberturvalisuse nõuetele, ning seoses Euroopa digiidentiteedikukrutega seotud muude kui küberturvalisuse nõuetega, peaksid liikmesriigid kehtestama riiklikud sertifitseerimiskavad, tehes seda vastavalt käesolevas määruses sätestatud ja selle kohaselt vastu võetud ühtlustatud nõuetele. Liikmesriigid peaksid edastama oma riiklike sertifitseerimiskavade kavandid Euroopa digiidentiteedi koostöörühmale, kellel peaks olema võimalus esitada arvamusi ja soovitusi.

(25) Käesolevas määruses sätestatud küberturvalisuse nõuetele vastavuse sertifitseerimine peaks võimaluse korral tuginema asjakohastele Euroopa küberturvalisuse sertifitseerimise kavadele, mis on kehtestatud vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2019/881[10], millega kehtestatakse IKT toodete, protsesside ja teenuste Euroopa küberturvalisuse sertifitseerimise vabatahtlik raamistik.

---

[10] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

(26) Selleks et pidevalt hinnata ja leevendada turvalisusega seotud riske, tuleks sertifitseeritud Euroopa digiidentiteedikukrute suhtes korrapäraselt läbi viia nõrkuste hindamised, mille eesmärk on tuvastada Euroopa digiidentiteedikukru sertifitseeritud toodete, protsesside ja teenustega seotud komponentide nõrkusi.

(27) Käesolevas määruses sätestatud olulised küberturvalisuse nõuded kaitsevad kasutajaid ja ettevõtteid küberriskide eest ning aitavad ühtlasi parandada isikuandmete kaitset ja üksikisikute privaatsust. Komisjoni, Euroopa standardiorganisatsioonide, Euroopa Liidu Küberturvalisuse Ameti (ENISA), määrusega (EL) 2016/679 loodud Euroopa Andmekaitsenõukogu ja riiklike andmekaitse järelevalveasutuste vahelises koostöös tuleks kaaluda koostoimet nii küberturvalisuse aspektide standardimise kui ka sertifitseerimise vallas.

(28) Euroopa digiidentiteedikukru aktiveerimist tuleks hõlbustada liidu kodanike ja elanike jaoks, tuginedes kõrgel usaldusväärsuse tasemel väljastatud e-identimise vahenditele. Märkimisväärsel usaldusväärsuse tasemel väljastatud e-identimise vahenditele tuleks tugineda ainult juhul, kui märkimisväärsel usaldusväärsuse tasemel väljastatud e-identimise vahendeid kasutavad ühtlustatud tehnilised kirjeldused ja menetlused koos täiendavate identiteedi kontrollimise vahenditega võimaldavad täita käesolevas määruses kõrge usaldusväärsuse tasemega seoses sätestatud nõudeid. Sellised täiendavad vahendid peaksid olema usaldusväärsed ja kergesti kasutatavad ning need võiksid tugineda võimalusele kasutada kaugaktiveerimismenetlust, kvalifitseeritud e-allkirjadega toetatavaid kvalifitseeritud sertifikaate, kvalifitseeritud elektroonilisi tõendeid või nende kombinatsiooni. Selleks et tagada Euroopa digiidentiteedikukrute piisav kasutuselevõtt, tuleks rakendusaktides sätestada ühtlustatud tehnilised kirjeldused ja menetlused teenuse kasutajate jaoks aktiveerimiseks e-identimise vahendite, sealhulgas märkimisväärsel usaldusväärsuse tasemel väljastatud vahendite abil.

(29) Käesoleva määruse eesmärk on pakkuda kasutajale täielikult mobiilset, turvalist ja kasutajasõbralikku Euroopa digiidentiteedikukrut. Kuni sertifitseeritud võltsimiskindlate lahenduste, näiteks kasutajate seadmetes sisalduvate turvaelementide kättesaadavuseni peaksid Euroopa digiidentiteedikukrud olema üleminekumeetmena võimelised tuginema sertifitseeritud välistele turvaelementidele krüptomaterjali ja muude tundlike andmete kaitsmisel või teavitatud e-identimise vahenditele kõrgel usaldusväärsuse tasemel, et tõendada vastavust käesoleva määruse asjakohastele nõuetele seoses Euroopa digiidentiteedikukru usaldusväärsuse tasemega. Kui üleminekumeede tugineb sertifitseeritud välisele turvaelemendile, ei tohiks käesolev määrus piirata selle väljastamise ja kasutamise riigisiseste tingimuste kohaldamist.

(30) Euroopa digiidentiteedikukrud peaksid tagama avalikele ja erasektori teenustele juurdepääsu hõlbustamiseks vajaliku e-identimise ja e-autentimise läbiviimisel kasutatavate andmete kaitse ja turvalisuse kõrgeimal tasemel, olenemata sellest, kas neid andmeid säilitatakse lokaalselt või pilvepõhistes lahendustes, võttes igakülgselt arvesse erinevaid riskitasemeid.

(31) Euroopa digiidentiteedikukrud peaksid olema lõimitud turbega ja peaksid rakendama täiustatud turvaelemente, et kaitsta identiteedivarguse, muu andmevarguse, teenusetõkestuse ja muude küberohtude eest. See turvalisus peaks hõlmama tipptasemel krüpteerimis- ja salvestusmeetodeid, mis on kättesaadavad üksnes kasutajale ja mida üksnes kasutaja saab dekrüpteerida, ning mis tuginevad otspunktkrüpteeritud sidele teiste Euroopa digiidentiteedikukrute ja tuginevate isikutega. Lisaks peaksid Euroopa digiidentiteedikukrud nõudma turvalist, selget ja aktiivset kasutaja kinnitust Euroopa digiidentiteedikukrute kaudu tehtavate toimingute kohta.

(32) Euroopa digiidentiteedikukrute tasuta kasutamine ei tohiks kaasa tuua enamate andmete töötlemist, kui on vaja Euroopa digiidentiteedikukru teenuste osutamiseks. Käesolev määrus ei tohiks lubada Euroopa digiidentiteedikukru pakkujal töödelda muul eesmärgil kui Euroopa digiidentiteedikukru teenuste osutamiseks selliseid isikuandmeid, mis on salvestatud Euroopa digiidentiteedikukrusse või mis tulenevad Euroopa digiidentiteedikukru kasutamisest. Privaatsuse tagamiseks peaksid Euroopa digiidentiteedikukru pakkujad tagama mittejälgitavuse, mistõttu ei tohi nad koguda andmeid ega omada ülevaadet Euroopa digiidentiteedikukru kasutajate tehingute kohta. Selline mittejälgitavus tähendab, et kukru pakkujatel ei ole võimalik näha kasutaja tehtud tehingute üksikasju. Erijuhtudel, mis põhinevad kasutaja eelneval sõnaselgel nõusolekul iga konkreetse juhtumi puhul, ja täielikus kooskõlas määrusega (EL) 2016/679, võib Euroopa digiidentiteedikukrute pakkujatele siiski anda juurdepääsu teabele, mida on vaja Euroopa digiidentiteedikukrutega seotud konkreetse teenuse osutamiseks.

(33) Euroopa digiidentiteedikukrute läbipaistvus ja nende pakkujate vastutus on sotsiaalse usalduse loomise ja raamistiku omaksvõtmise põhielemendid. Euroopa digiidentiteedikukrute toimimine peaks seetõttu olema läbipaistev ja eelkõige võimaldama isikuandmete kontrollitavat töötlemist. Selle saavutamiseks peaksid liikmesriigid avalikustama Euroopa digiidentiteedikukrute kasutajate rakendustarkvara komponentide lähtekoodi, sealhulgas selliste komponentide lähtekoodi, mis on seotud isikuandmete ja juriidiliste isikute andmete töötlemisega. Selle lähtekoodi avaldamine avatud lähtekoodi litsentsi alusel peaks võimaldama ühiskonnal, sealhulgas kasutajatel ja arendajatel, mõista selle toimimist ning seda auditeerida ja läbi vaadata. See suurendaks kasutajate usaldust digiidentiteedikukru ökosüsteemi vastu ja Euroopa digiidentiteedikukrute turvalisust, võimaldades igaühel teatada koodi nõrkustest ja vigadest. Üldiselt peaks see andma tarnijatele stiimuleid pakkuda ja hoida töös toodet, mis on väga turvaline. Teatavatel juhtudel võivad liikmesriigid, kui see on igakülgselt põhjendatud, eelkõige avaliku julgeoleku huvides piirata kasutatud teekide, sidekanali või muude, kasutajaseadmes mittemajutatavate elementide lähtekoodi avalikustamist.

(34) Euroopa digiidentiteedikukrute kasutamine ja nende kasutamise lõpetamine peaks olema kasutajate ainuõigus ja valik. Liikmesriigid peaksid välja töötama lihtsa ja turvalise menetluse, et kasutajad saaksid taotleda Euroopa digiidentiteedikukrute kehtivuse viivitamatut kehtetuks tunnistamist, sealhulgas ka kaotuse või varguse korral. Seoses kasutaja surma või juriidilise isiku tegevuse lõpetamisega tuleks luua mehhanism, mis võimaldaks füüsilise isiku pärimisasjade või juriidilise isiku varaga seonduva lahendamise eest vastutaval asutusel või ametiisikul taotleda Euroopa digiidentiteedikukru viivitamatut kehtetuks tunnistamist.

(35) Selleks et edendada Euroopa digiidentiteedikukrute kasutuselevõttu ja digiidentiteedi laiemat kasutamist, peaksid liikmesriigid mitte ainult propageerima asjaomaste teenuste eeliseid, vaid peaksid töötama koostöös erasektori, teadlaste ja akadeemiliste ringkondadega välja ka koolitusprogrammid, mille eesmärk on tugevdada oma kodanike ja elanike digioskusi, eelkõige kaitsetute rühmade, näiteks puuetega inimeste ja eakate inimeste jaoks. Liikmesriigid peaksid ka suurendama teavituskampaaniate abil teadlikkust Euroopa digiidentiteedikukrute kasulikkusest ja nendega seotud riskidest.

(36) Et Euroopa digiidentiteedi raamistik oleks avatud innovatsioonile ja tehnoloogiaarendusele ning on tulevikukindel, innustatakse liikmesriike looma ühiselt testkeskkondi uuenduslike lahenduste testimiseks kontrollitud ja turvalises keskkonnas, eelkõige selleks, et parandada lahenduste funktsionaalsust, isikuandmete kaitset, turvalisust ja koostalitlusvõimet ning anda teavet tehniliste viidete ja õiguslike nõuete edaspidiseks ajakohastamiseks. Kõnealune keskkond peaks soodustama VKEde, iduettevõtjate, üksikisikutest novaatorite ja teadlaste ning asjaomaste tööstusharu sidusrühmade kaasamist. Sellised algatused peaksid aitama kaasa sellele, et liidu kodanikele ja elanikele pakutavad Euroopa digiidentiteedikukrud vastavad õigusnormidele ning on tehniliselt stabiilsed, samuti peaksid need algatused nõuetele vastavust ja tehnilist stabiilsust tugevdama, vältides seeläbi selliste lahenduste väljatöötamist, mis ei ole kooskõlas liidu andmekaitsealase õigusega või mis põhjustavad turvaauke.

(37) Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/1157[11] suurendatakse 2021. aasta augustiks isikutunnistuste turvalisust täiustatud turvaelementidega. Liikmesriigid peaksid kaaluma võimalust teatada neist e-identimise süsteemide raames, et laiendada e-identimise vahendite piiriülest kättesaadavust.

(38) E-identimise süsteemidest teatamise korda tuleks lihtsustada ja kiirendada, et edendada juurdepääsu hõlpsasti kasutatavatele, usaldusväärsetele, turvalistele ja uuenduslikele autentimis- ja identimislahendustele ning asjakohasel juhul julgustada eraõiguslikke identiteedilahenduste tarnijaid pakkuma liikmesriikide ametiasutustele e-identimise süsteeme, millest teatada määruse (EL) nr 910/2014 kohaselt kui riiklikest e-identimise süsteemidest.

(39) Olemasolevate teatamis- ja vastastikuse hindamise menetluste ühtlustamine väldib ebaühtlast lähenemist erinevate teavitatud e-identimise süsteemide hindamisele ja hõlbustab usalduse suurendamist liikmesriikide vahel. Uute, lihtsustatud mehhanismide eesmärk on edendada liikmesriikide koostööd nende teavitatud e-identimise süsteemide turvalisuse ja koostalitlusvõime valdkonnas.

(40) Liikmesriikidel peaksid olema uued, paindlikud vahendid, et tagada käesoleva määruse ja selle alusel vastu võetud asjakohaste rakendusaktide nõuete täitmine. Käesolev määrus peaks võimaldama liikmesriikidel kasutada akrediteeritud vastavushindamisasutuste koostatud aruandeid ja hinnanguid, mis on ette nähtud määruse (EL) 2019/881 alusel liidu tasandil kehtestatavate sertifitseerimise kavade kontekstis, et toetada oma väiteid selle kohta, et kavad või nende osad on kooskõlas määrusega (EL) nr 910/2014.

---

[11] Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta määrus (EL) 2019/1157 liidu kodanike isikutunnistuste ning vaba liikumise õigust kasutavatele liidu kodanikele ja nende pereliikmetele väljaantavate elamislubade turvalisuse suurendamise kohta (ELT L 188, 12.7.2019, lk 67).

(41) Avalike teenuste osutajad kasutavad määruse (EL) nr 910/2014 kohastest e-identimise vahenditest kättesaadavaid isikutuvastusandmeid, et ühitada teisest liikmesriigist pärit kasutajate e-identiteet isikutuvastusandmetega, mis omistatakse sellistele kasutajatele liikmesriigis, mis viib läbi piiriülest identiteedi ühitamise protsessi. Hoolimata teavitatud e-identimise süsteemide raames esitatud minimaalse andmekogumi kasutamisest tuleb paljudel juhtudel identiteedi ühitamise täpsuse tagamiseks juhul, kui liikmesriigid tegutsevad tuginevate isikutena, saada lisateavet kasutaja kohta ja riiklikul tasandil viia läbi konkreetseid täiendavaid menetlusi üheseks identimiseks. Selleks et veelgi toetada e-identimise vahendite kasutatavust, pakkuda paremaid internetipõhiseid avalikke teenuseid ja suurendada õiguskindlust seoses kasutajate e-identiteediga, tuleks määrusega (EL) nr 910/2014 nõuda liikmesriikidelt konkreetsete internetipõhiste meetmete võtmist, et tagada identiteedi ühene ühitamine, kui kasutajad kavatsevad saada ligipääsu piiriülestele avalikele teenustele internetis.

(42) Euroopa digiidentiteedikukrute väljatöötamisel tuleb arvesse võtta kasutajate vajadusi. Tuleks teha kättesaadavaks Euroopa digiidentiteedikukrutel põhinevad sisukad kasutusjuhud ja internetipõhised teenused. Kasutajate mugavuse huvides ja selliste teenuste piiriülese kättesaadavuse tagamiseks on oluline võtta meetmeid, et soodustada sarnase käsituse kohaldamist internetipõhiste teenuste kavandamise, arendamise ja rakendamise suhtes kõigis liikmesriikides. Selle eesmärgi saavutamiseks võiks olla kasu mittesiduvatest suunistest Euroopa digiidentiteedikukrutel põhinevate internetipõhiste teenuste kavandamise, arendamise ja rakendamise kohta. Selliste suuniste koostamisel tuleks arvesse võtta liidu koostalitlusvõime raamistikku. Liikmesriikidel peaks olema suuniste vastuvõtmisel juhtroll.

(43) Kooskõlas Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2019/882[12] ja ÜRO puuetega inimeste õiguste konventsiooniga peaksid puuetega inimesed saama kasutada Euroopa digiidentiteedikukruid, usaldusteenuseid ja nende teenuste osutamisel kasutatavaid lõpptarbijale suunatud tooteid teiste kasutajatega võrdsetel alustel.

(44) Käesoleva määruse tõhusa täitmise tagamiseks tuleks nii kvalifitseeritud kui ka kvalifitseerimata usaldusteenuse osutajatele kehtestada maksimaalsete haldustrahvide miinimummäärad. Liikmesriigid peaksid kehtestama mõjusad, proportsionaalsed ja hoiatavad karistused. Karistuste kindlaksmääramisel tuleks igakülgselt arvesse võtta mõjutatud üksuste suurust, nende ärimudeleid ja rikkumiste tõsidust.

(45) Liikmesriigid peaksid kehtestama karistusnormid selliste rikkumiste puhuks nagu otsene või kaudne tegevus, mis põhjustab kvalifitseerimata ja kvalifitseeritud usaldusteenuste segiajamist või ELi usaldusmärgi kuritarvitamist kvalifitseerimata usaldusteenuse osutajate poolt. ELi usaldusmärki ei tohiks kasutada tingimustel, mis otse või kaudselt viivad arusaamani, et mis tahes selliste teenuseosutajate pakutavad kvalifitseerimata usaldusteenused on kvalifitseeritud.

(46) Käesolev määrus ei peaks hõlmama lepingute sõlmimise ja kehtivusega või muude õiguslike kohustuste tekkimise ja kehtivusega seotud aspekte, kui vorminõuded on sätestatud liidu või riigisiseses õiguses. Samuti ei peaks käesolev määrus mõjutama riigisiseseid vorminõudeid avalike registrite, eelkõige äriregistri ja kinnistusraamatu kohta.

---

[12] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta direktiiv (EL) 2019/882 toodete ja teenuste ligipääsetavusnõuete kohta (ELT L 151, 7.6.2019, lk 70).

(47) Usaldusteenuste osutamine ja kasutamine ning kasu, mida saadakse piiriüleste tehingute mugavuse ja õiguskindluse tulemusel, eelkõige kvalifitseeritud usaldusteenuste kasutamise korral, muutuvad rahvusvahelises kaubanduses ja koostöös üha olulisemaks. Liidu rahvusvahelised partnerid loovad määrusest (EL) nr 910/2014 ajendatud usaldusraamistikke. Kvalifitseeritud usaldusteenuste ja nende osutajate tunnustamise hõlbustamiseks võib komisjon võtta vastu rakendusakte, et kehtestada tingimused, mille alusel võib kolmandate riikide usaldusraamistikke pidada samaväärseks käesolevas määruses sätestatud kvalifitseeritud usaldusteenuste ja nende teenuseosutajate usaldusraamistikuga. Selline käsitus peaks täiendama liidu ja kolmandate riikide usaldusteenuste ning liidus ja kolmandates riikides asutatud teenuseosutajate vastastikuse tunnustamise võimalust kooskõlas Euroopa Liidu toimimise lepingu (ELi toimimise leping) artikliga 218. Kui kehtestatakse tingimused, mille alusel võib kolmandate riikide usaldusraamistikke pidada samaväärseks määruses (EL) nr 910/2014 sätestatud kvalifitseeritud usaldusteenuste ja nende teenuseosutajate usaldusraamistikuga, tuleks tagada vastavus Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555[13] ning määruse (EL) 2016/679 asjakohastega sätetega ning usaldusnimekirjade kui usalduse loomise oluliste elementide kasutamine.

[13] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80).

(48) Käesolev määrus peaks edendama võimalust valida ja vahetada Euroopa digiidentiteedikukruid, kui liikmesriik on oma territooriumil heaks kiitnud rohkem kui ühe Euroopa digiidentiteedikukru lahenduse. Selleks et vältida sellistes olukordades ühe lahenduse kinnistumist, peaksid Euroopa digiidentiteedikukrute pakkujad, kui see on tehniliselt teostatav, tagama andmete tõhusa ülekantavuse Euroopa digiidentiteedikukru kasutajate taotlusel ning neil ei tohiks olla lubatud kasutada lepingulisi, majanduslikke või tehnilisi tõkkeid, et vältida või takistada Euroopa digiidentiteedikukrute tõhusat vahetamist.

(49) Euroopa digiidentiteedikukrute nõuetekohase toimimise tagamiseks vajavad Euroopa digiidentiteedikukrute pakkujad toimivat koostalitlusvõimet ning õiglasi, mõistlikke ja mittediskrimineerivaid tingimusi, et Euroopa digiidentiteedikukrud saaksid kasutada mobiilseadmete konkreetseid riist- ja tarkvaraelemente. Need komponendid võiksid hõlmata eelkõige lähiväljaside antenne ja turvaelemente, sealhulgas universaalsed kiipkaardid, sisseehitatud turvaelemendid, mikroSD kaardid ja Bluetoothi madala energiatarbega protokoll. Juurdepääs nendele komponentidele võib olla mobiilsideoperaatorite ja seadmete tootjate kontrolli all. Seepärast ei tohiks mobiilseadmete originaalseadmete tootjad ega elektroonilise side teenuste osutajad keelata juurdepääsu sellistele komponentidele, kui seda on vaja Euroopa digiidentiteedikukrute teenuste osutamiseks. Lisaks tuleks nende ettevõtjate suhtes, kes on määratud põhiplatvormiteenuste pääsuvalitsejateks ja kelle komisjon on kandnud loetellu vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2022/1925,[14] jätkuvalt kohaldada kõnealuse määruse erisätteid, tuginedes nimetatud määruse artikli 6 lõikele 7.

---

[14] Euroopa Parlamendi ja nõukogu 14. septembri 2022. aasta määrus (EL) 2022/1925, mis käsitleb konkurentsile avatud ja õiglaseid turge digisektoris ning millega muudetakse direktiive (EL) 2019/1937 ja (EL) 2020/1828 (digiturgude määrus) (ELT L 265, 12.10.2022, lk 1).

(50) Et ühtlustada usaldusteenuse osutajatele pandud küberturvalisuse kohustusi ning võimaldada neil teenuseosutajatel ja nende vastavatel pädevatel asutustel kohaldada direktiiviga (EL) 2022/2555 kehtestatud õigusraamistikku, peavad usaldusteenuse osutajad võtma kõnealuse direktiivi kohaselt asjakohaseid tehnilisi ja korralduslikke meetmeid, näiteks võtma meetmeid süsteemitõrgete, inimvigade, pahatahtliku tegevuse või loodusnähtuste käsitlemiseks, et juhtida riske, mis ohustavad selliste võrgu- ja infosüsteemide turvalisust, mida need teenuseosutajad kasutavad oma teenuste osutamisel, ning teatama olulistest intsidentidest ja küberohtudest kooskõlas kõnealuse direktiiviga. Mis puutub intsidentidest teatamisse, siis peaksid usaldusteenuse osutajad teatama kõigist intsidentidest, millel on oluline mõju nende teenuste osutamisele, sealhulgas sellistest intsidentidest, mis on põhjustatud seadmete vargusest või kaotsiminekust, võrgukaabli kahjustustest või isiku tuvastamise käigus toimunud intsidentidest. Direktiivi (EL) 2022/2555 kohaseid küberriskide juhtimise nõudeid ja teatamiskohustusi tuleks käsitada käesoleva määrusega usaldusteenuse osutajate suhtes kehtestatud nõuete täiendusena. Direktiivi (EL) 2022/2555 kohaselt määratud pädevad asutused peaksid asjakohasel juhul jätkuvalt kohaldama väljakujunenud riiklikke tavasid või suuniseid seoses turva- ja aruandlusnõuete rakendamisega ning selliste nõuete täitmise järelevalvega vastavalt määrusele (EL) nr 910/2014. Käesolev määrus ei piira kohustust teatada isikuandmetega seotud rikkumistest vastavalt määrusele (EL) 2016/679.

(51) Igapidi tuleks arvesse võtta toimiva koostöö tagamist määruse (EL) nr 910/2014 artikli 46b kohaselt määratud järelevalveasutuste ja direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud või asutatud pädevate asutuste vahel. Kui selline järelevalveasutus erineb sellisest pädevast asutusest, peaksid nad tegema tihedat ja õigeaegset koostööd, vahetades asjakohast teavet, et tagada tulemuslik järelevalve ja usaldusteenuse osutajate vastavus määruses (EL) nr 910/2014 ja direktiivis (EL) 2022/2555 sätestatud nõuetele. Eelkõige peaks määruse (EL) nr 910/2014 kohaselt määratud järelevalveasutustel olema õigus nõuda direktiivi (EL) 2022/2555 kohaselt määratud või asutatud pädevalt asutuselt, et ta esitaks kvalifitseeritud staatuse andmiseks vajaliku asjakohase teabe ja võtaks järelevalvemeetmeid, et kontrollida, kas usaldusteenuse osutajad täidavad direktiivi (EL) 2022/2555 asjakohaseid nõudeid, või nõuda, et nad kõrvaldaksid mittevastavuse.

(52) Oluline on luua õigusraamistik registreeritud e-andmevahetusteenusega seotud olemasolevate riiklike õigussüsteemide piiriülese tunnustamise hõlbustamiseks. Selline raamistik võiks avada liidu usaldusteenuse osutajatele uued turuvõimalused ka uute kogu liitu hõlmavate registreeritud e-andmevahetusteenuste pakkumisel. Selle tagamiseks, et kvalifitseeritud registreeritud e-andmevahetusteenust kasutades edastatakse andmed õigele adressaadile, peaksid kvalifitseeritud registreeritud e-andmevahetusteenused tagama adressaadi tuvastamise täieliku kindluse, samal ajal kui saatja identifitseerimine vajaks kõrget usaldusväärsuse taset. Liikmesriigid peaksid julgustama kvalifitseeritud registreeritud e-andmevahetusteenuste osutajaid muutma oma teenused koostalitlusvõimeliseks teiste kvalifitseeritud usaldusteenuse osutajate osutatavate kvalifitseeritud registreeritud e-andmevahetusteenustega, et elektrooniliselt registreeritud andmeid ladusalt kahe või enama kvalifitseeritud usaldusteenuse osutaja vahel edastada ja siseturul õiglasi tavasid edendada.

(53) Enamikul juhtudel ei ole liidu kodanikel ja elanikel võimalik piiriüleselt, turvaliselt ja kõrgetasemelise andmekaitse tingimustes vahetada digitaalselt sellist oma identiteediga seotud teavet nagu aadress, vanus, kutsekvalifikatsioon, juhiluba ja muud load ning makseandmed.

(54) Peaks olema võimalik väljastada ja hallata usaldusväärseid elektroonilisi atribuute ning aidata vähendada halduskoormust, andes liidu kodanikele ja elanikele võimaluse kasutada neid oma era- ja avaliku sektori tehingutes. Liidu kodanikel ja elanikel peaks näiteks olema võimalik tõendada, et neil on ühe liikmesriigi ametiasutuse väljastatud kehtiv juhiluba, mida teiste liikmesriikide asjaomased ametiasutused saavad kontrollida ja millele nad võivad tugineda, ning kasutada piiriüleses kontekstis oma sotsiaalkindlustusõigusi või tulevasi elektroonilisi reisidokumente.

(55) Elektrooniliste tõendite usaldusteenuse pakkujana tuleks käsitada iga teenuseosutajat, kes väljastab elektroonilisi tõendeid, nagu diplomid, litsentsid, sünnitunnistused või füüsiliste või juriidiliste isikute esindamise volitused. Elektroonilist tõendit ei tohiks tunnistada õiguslikult kehtetuks seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud elektroonilistele tõenditele esitatavatele nõuetele. Tuleks sätestada üldnõuded, millega tagatakse, et kvalifitseeritud elektroonilisel tõendil on seaduslikult väljastatud paberil tõenditega samaväärne õiguslik toime. Neid nõudeid tuleks kohaldada, ilma et see piiraks sellise liidu või riigisisese õiguse kohaldamist, millega määratakse kindlaks täiendavad sektoripõhised vorminõuded, millel on õiguslik toime, ja eelkõige kvalifitseeritud elektrooniliste tõendite piiriülest tunnustamist, kui see on asjakohane.

(56) Euroopa digiidentiteedikukrute laialdane kättesaadavus ja kasutatavus peaks suurendama nende omaksvõttu ja usaldust nende vastu nii eraisikute kui ka eraõiguslike teenuseosutajate seas. Erasektori tuginevad isikud, kes osutavad teenuseid näiteks transpordi, energia, pangandus- ja finantsteenuste, sotsiaalkindlustuse, tervishoiu, joogivee, postiteenuste, digitaristu, telekommunikatsiooni või hariduse valdkonnas, peaksid seetõttu aktsepteerima Euroopa digiidentiteedikukrute kasutamist selliste teenuste osutamisel, mille puhul nõutakse liidu või riigisisese õiguse või lepinguliste kohustuste alusel e-identimise korral tugevat kasutaja autentimist. Kõik tugineva isiku teabepäringud Euroopa digiidentiteedikukru kasutajalt peaksid olema vajalikud ja proportsionaalsed konkreetse juhtumi puhul kavandatud kasutusega, peaksid olema kooskõlas võimalikult väheste andmete kogumise põhimõttega ja peaksid tagama läbipaistvuse seoses sellega, milliseid andmeid jagatakse ja mis eesmärgil. Euroopa digiidentiteedikukrute kasutamise ja omaksvõtu hõlbustamiseks tuleks kukrute kasutuselevõtmisel arvesse võtta laialdaselt tunnustatud valdkondlikke standardeid ja kirjeldusi.

(57) Kui väga suured digiplatvormid Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2065[15] artikli 33 lõike 1 tähenduses nõuavad kasutajatelt enda autentimist, et saada juurdepääs internetipõhistele teenustele, peaks neil platvormidel olema kohustus aktsepteerida kasutaja vabatahtliku taotluse korral Euroopa digiidentiteedikukrute kasutamist. Kasutajatel ei tohiks olla kohustust kasutada erasektori teenustele juurdepääsuks Euroopa digiidentiteedikukrut ning nende juurdepääsu teenustele ei tohiks piirata ega takistada põhjusel, et nad ei kasuta Euroopa digiidentiteedikukrut. Kui aga kasutajad seda soovivad, peaksid väga suured digiplatvormid neid sel eesmärgil aktsepteerima, järgides võimalikult väheste andmete kogumise põhimõtet ja kasutajate õigust kasutada vabalt valitud varjunime. Võttes arvesse seda, kui tähtsat rolli mängivad väga suured digiplatvormid nende haardeulatuse tõttu, mis väljendub eelkõige teenusesaajate ja majandustehingute hulgas, on Euroopa digiidentiteedikukrute aktsepteerimise kohustus vajalik, et suurendada kasutajate kaitset pettuste eest ja tagada kõrgetasemeline andmekaitse.

(58) Välja tuleks töötada liidu tasandi tegevusjuhendid, et soodustada e-identimise vahendite, sealhulgas käesoleva määruse kohaldamisalasse kuuluvate Euroopa digiidentiteedikukrute laialdast kättesaadavust ja kasutatavust. Tegevusjuhendid peaksid hõlbustama e-identimise vahendite, sealhulgas Euroopa digiidentiteedikukrute aktsepteerimist selliste teenuseosutajate poolt, kes ei kvalifitseeru väga suurteks digiplatvormideks ja kes tuginevad kasutajate autentimisel kolmandate isikute e-identimise teenustele.

---

[15] Euroopa Parlamendi ja nõukogu 19. oktoobri 2022. aasta määrus (EL) 2022/2065, mis käsitleb digiteenuste ühtset turgu ja millega muudetakse direktiivi 2000/31/EÜ (digiteenuste määrus) (ELT L 277, 27.10.2022, lk 1).

(59) Valikuline avaldamine on kontseptsioon, mis annab andmete omanikule õiguse avaldada ainult osa suuremast andmekogumist, et andmeid saav üksus saaks ainult sellist teavet, mida on vaja kasutaja soovitud teenuse osutamiseks. Euroopa digiidentiteedikukkur peaks tehniliselt võimaldama atribuutide valikulist avaldamist tuginevatele isikutele. Kasutajal peaks olema tehniliselt võimalik atribuute valikuliselt avaldada, sealhulgas mitme erineva elektroonilise tõendi atribuute, ning neid kombineerida ja sujuvalt tuginevatele isikutele esitada. See funktsioon peaks muutuma Euroopa digiidentiteedikukrute põhiomaduseks, mis suurendab mugavust ja isikuandmete kaitset, sealhulgas tagab võimalikult väheste andmete kogumise.

(60) Välja arvatud juhul, kui liidu või riigisisesed õigusnormid nõuavad kasutajate identimist, ei tohiks keelata juurdepääsu teenustele varjunime kasutades.

(61) Kvalifitseeritud usaldusteenuse osutajate poolt kvalifitseeritud tõendi osana pakutavaid atribuute peaksid autentsetest allikatest kontrollima kas kvalifitseeritud usaldusteenuse osutajad otse või määratud vahendajate abil, kes on vastavalt liidu või riigisisesele õigusele tunnustatud riiklikul tasandil tegema tõendatud atribuutide turvalist vahetamist identiteedi või atribuutide tõendamisteenuse osutajate ja tuginevate isikute vahel. Liikmesriigid peaksid riiklikul tasandil kehtestama asjakohased mehhanismid tagamaks, et kvalifitseeritud elektroonilist tõendit väljastavad kvalifitseeritud usaldusteenuse osutajad saavad selle isiku nõusolekul, kellele tõend on väljastatud, kontrollida atribuutide autentsust, tuginedes autentsetele allikatele. Asjakohastel mehhanismidel peaks olema võimalik hõlmata konkreetsete vahendajate või tehniliste lahenduste kasutamist kooskõlas riigisisese õigusega, mis võimaldab juurdepääsu autentsetele allikatele. Sellise mehhanismi kättesaadavuse tagamine, mis võimaldab atribuutide kontrollimist autentsete allikate alusel eesmärk on hõlbustada kvalifitseeritud elektrooniliste tõenditega tegelevate kvalifitseeritud usaldusteenuse osutajate määruses (EL) nr 910/2014 sätestatud kohustuste täitmist. Kõnealuse määruse uus lisa peaks sisaldama nende atribuudikategooriate loetelu, mille puhul liikmesriigid peavad tagama, et võetakse meetmeid, mis võimaldavad kvalifitseeritud elektrooniliste tõendite pakkujatel kasutaja taotlusel kontrollida elektrooniliselt nende autentsust asjakohase autentse allika alusel.

(62) Turvaline e-identimine ja atribuutide tõendamine peaks pakkuma finantsteenuste sektorile täiendavat paindlikkust ja lahendusi, mis võimaldavad identida kliente ja vahetada konkreetseid atribuute, mida on vaja näiteks selleks, et täita tulevase Rahapesu ja Terrorismi Rahastamise Tõkestamise Ameti loomist käsitleva tulevase määruse kohaseid kliendi suhtes rakendatavaid hoolsuskohustuse nõudeid, investorite kaitset käsitlevast õigusest tulenevaid sobivusnõudeid, või selleks, et makseteenuste valdkonnas toetada kontole sisselogimise ja tehingute algatamise eesmärgil toimuva e-identimise puhul kliendi tugeva autentimise nõuete täitmist.

(63) E-allkirja õiguslikku toimet ei saa vaidlustada põhjusel, et see on elektroonilisel kujul või et see ei vasta kvalifitseeritud e-allkirja nõuetele. E-allkirjade õiguslik toime tuleb kindlaks määrata riigisiseses õiguses, välja arvatud käesolevas määruses sätestatud nõue, mille kohaselt kvalifitseeritud e-allkirja õiguslik toime loetakse käsitsi kirjutatud allkirjaga samaväärseks. E-allkirjade õigusliku toime kindlaksmääramisel peaksid liikmesriigid arvesse võtma allkirjastatava dokumendi õigusliku väärtuse ning e-allkirja nõutava turvalisuse taseme ja kulude proportsionaalsuse põhimõtet. E-allkirjade kättesaadavuse ja kasutamise edendamiseks julgustatakse liikmesriike kaaluma igapäevastes tehingutes täiustatud e-allkirjade kasutamist, kuna need tagavad piisaval tasemel turvalisuse ja usaldusväärsuse.

(64) Sertifitseerimistavade ühtsuse tagamiseks kogu liidus peaks komisjon välja andma suunised kvalifitseeritud e-allkirja andmise vahendite ja kvalifitseeritud e-templi loomise vahendite sertifitseerimise ja uuesti sertifitseerimise kohta, sealhulgas nende kehtivuse ja ajaliste piirangute kohta. Käesolev määrus ei takista avalik-õiguslikel või eraõiguslikel asutustel, kellel on sertifitseeritud kvalifitseeritud e-allkirja andmise vahendid, neid vahendeid ajutiselt uuesti sertifitseerimast lühiajaliseks sertifitseerimisperioodiks, võttes aluseks viimase sertifitseerimise tulemused, kui sellist sertifitseerimist ei ole võimalik õiguslikult kehtestatud aja jooksul uuesti teha muul põhjusel kui turvarikkumise või turvaintsidendi tõttu, ilma et see piiraks kohaldatavat sertifitseerimistava.

(65) Veebisaidi autentimise sertifikaatide väljastamine tagab kasutajatele kõrgel usaldusväärsuse tasemel andmed veebisaiti käitava üksuse identiteedi kohta, seda sõltumata sellest, millisel platvormil identiteeti kuvatakse. Sellised sertifikaadid peaksid aitama luua usaldust internetipõhise äritegevuse vastu, kuna autenditud veebisait on kasutajate jaoks usaldusväärne. Selliste sertifikaatide kasutamine peaks veebisaitide jaoks olema vabatahtlik. Selleks, et veebisaidi autentimisest saaks usalduse suurendamise, kasutajakogemuse parandamise ja majanduskasvu suurendamise vahend siseturul, sätestatakse käesolevas määruses usaldusraamistik, mis hõlmab kvalifitseeritud veebisaidi autentimise sertifikaatide pakkujate minimaalseid turvalisuse ja vastutusega seotud kohustusi ning nende sertifikaatide väljastamise tingimusi. Riigisisesed usaldusnimekirjad peaksid kinnitama veebisaidi autentimisteenuste ja nende usaldusteenuse osutajate kvalifitseeritud staatust, sealhulgas nende täielikku vastavust käesoleva määruse nõuetele seoses veebisaidi autentimise kvalifitseeritud sertifikaatide väljastamisega. Veebisaidi autentimise kvalifitseeritud sertifikaatide tunnustamine tähendab, et veebibrauserite pakkujad ei tohiks keelduda veebisaidi autentimise kvalifitseeritud sertifikaatide autentsuse tunnustamisest vaid selleks, et tõendada seost veebisaidi domeeninime ja selle füüsilise või juriidilise isiku vahel, kellele sertifikaat on väljastatud, või kinnitada selle isikusamasust. Veebibrauserite pakkujad peaksid lõppkasutajale kuvama enda valitud tehniliste vahenditega sertifitseeritud identiteediandmed ja muud tõendatud atribuudid kasutajasõbralikul viisil veebibrauseri keskkonnas. Selleks peaksid veebibrauserite pakkujad tagama toetuse ja koostalitlusvõime veebisaidi autentimise kvalifitseeritud sertifikaatidega, mis on väljastatud käesoleva määruse nõudeid täielikult järgides.

Veebisaidi autentimise kvalifitseeritud sertifikaatide tunnustamise ja koostalitlusvõime ning toetamise kohustus ei mõjuta veebibrauserite pakkujate vabadust tagada veebiturvalisus, domeeni autentimine ja veebiliikluse krüpteerimine viisil ja tehnoloogia abil, mida nad peavad kõige sobivamaks. Selleks et aidata kaasa lõppkasutajate turvalisusele internetis, peaks veebibrauserite pakkujatel olema erandkorras võimalik võtta ettevaatusabinõusid, mis on vajalikud ja proportsionaalsed, et reageerida tuvastatud sertifikaadi või sertifikaatide kogumi turvarikkumise või tervikluse kadumisega seotud põhjendatud muredele. Kui veebibrauserite pakkujad võtavad selliseid ettevaatusabinõusid, peaksid nad põhjendamatu viivituseta teavitama komisjoni, riiklikku järelevalveasutust ja üksust, kellele sertifikaat väljastati, ja kõnealuse sertifikaadi või sertifikaatide kogumi väljastanud kvalifitseeritud usaldusteenuse osutajat igast turvarikkumisest või tervikluse kadumisest ning ühe sertifikaadi või sertifikaatide kogumiga seoses võetud meetmetest. Nimetatud abinõud ei tohiks piirata veebibrauserite pakkujate kohustust tunnustada veebisaidi autentimise kvalifitseeritud sertifikaate kooskõlas riigisiseste usaldusnimekirjadega. Selleks et veelgi enam kaitsta liidu kodanikke ja elanikke ning edendada veebisaidi autentimise kvalifitseeritud sertifikaatide kasutamist, peaksid liikmesriikide ametiasutused kaaluma veebisaidi autentimise kvalifitseeritud sertifikaatide lisamist oma veebisaitidele. Käesolevas määruses sätestatud meetmed, mille eesmärk on suurendada sidusust liikmesriikide eri käsituste ja tavade vahel seoses järelevalvemenetlustega, on ette nähtud selleks, et suurendada usaldust ja kindlustunnet veebisaidi autentimise kvalifitseeritud sertifikaatide turvalisuse, kvaliteedi ja kättesaadavuse vastu.

(66) Paljud liikmesriigid on kehtestanud riiklikud nõuded elektroonilise arhiveerimise teenuste turvalisusele ja usaldusväärsusele, et võimaldada elektrooniliste andmete ja e-dokumentide ning nendega seotud usaldusteenuste pikaajalist säilitamist. Õiguskindluse, usalduse ja ühtlustamise tagamiseks kõigis liikmesriikides tuleks kehtestada kvalifitseeritud elektroonilise arhiveerimise teenuste õigusraamistik, mis oleks inspireeritud muude käesolevas määruses sätestatud usaldusteenuste raamistikust. Kvalifitseeritud elektroonilise arhiveerimise teenuste õigusraamistik peaks olema usaldusteenuse osutajatele ja kasutajatele tõhus töövahend, mis sisaldab elektroonilise arhiveerimise teenuse funktsionaalseid nõudeid ja kvalifitseeritud elektroonilise arhiveerimise teenuse kasutamisest tulenevaid selgeid õiguslikke tagajärgi. Neid sätteid tuleks kohaldada nii elektrooniliste andmete ja digitaalselt koostatud e-dokumentide kui ka skaneeritud ja digiteeritud paberdokumentide suhtes. Vajaduse korral peaksid need sätted võimaldama säilitatavate elektrooniliste andmete ja e-dokumentide portimist teistsugustele andmekandjatele või teistsugustesse vormingutesse, et tagada nende säilivus ja loetavus ka pärast nende tehnoloogilise kehtivusaja lõppemist, vältides samal ajal võimalikult suures ulatuses andmete kaotsiminekut ja muutmist. Kui elektroonilise arhiveerimise teenusele esitatud elektroonilised andmed ja e-dokumendid sisaldavad ühte või mitut kvalifitseeritud e-allkirja või kvalifitseeritud e-templit, tuleks teenuse puhul kasutada menetlusi ja tehnoloogiaid, millega on võimalik pikendada nende usaldusväärsust selliste andmete säilitusajaks, tuginedes võimaluse korral muude käesoleva määrusega loodud kvalifitseeritud usaldusteenuste kasutamisele. Säilitamistõendite loomiseks e-allkirjade, e-templite või e-ajatemplite kasutamise korral tuleks kasutada kvalifitseeritud usaldusteenuseid. Niivõrd kui elektroonilise arhiveerimise teenused ei ole käesoleva määrusega ühtlustatud, peaks liikmesriikidel olema võimalik kooskõlas liidu õigusega säilitada kõnealuseid teenuseid käsitlevad riigisisesed sätted või neid kehtestada, näiteks erisätted teenuste puhul, mis on integreeritud organisatsiooni ja mida kasutatakse üksnes kõnealuse organisatsiooni sisemiste arhiivide jaoks. Käesolevas määruses ei tohiks eristada elektroonilisi andmeid ja digitaalselt koostatud e-dokumente ning digiteeritud füüsilisi dokumente.

(67) Riiklike arhiivide ja mäluasutuste kui organisatsioonide, mis tegelevad dokumentaalpärandi säilitamisega avalikes huvides, tegevus on tavaliselt reguleeritud riigisisese õigusega ning nad ei pruugi osutada usaldusteenuseid käesoleva määruse tähenduses. Kui need asutused selliseid usaldusteenuseid ei osuta, ei piira käesolev määrus nende toimimist.

(68) Elektroonilised arvestusraamatud on elektrooniliste andmekirjete jada, mis peaksid tagama nende tervikluse ja kronoloogilise järjestuse täpsuse. Elektroonilised arvestusraamatud peaksid looma andmekirjete kronoloogilise järjestuse. Koos muude tehnoloogiatega peaksid need aitama leida lahendusi tõhusamateks ja murrangulisteks avalikeks teenusteks, nagu e-hääletamine, tolliasutuste piiriülene koostöö, akadeemiliste asutuste piiriülene koostöö ning kinnisvara omandiõiguse registreerimine detsentraliseeritud kinnistusregistrites. Kvalifitseeritud elektroonilised arvestusraamatud peaksid looma õigusliku eelduse registri andmekirjete kordumatu ja täpse kronoloogilise järjestuse ja tervikluse suhtes. Tulenevalt oma eripärast, nagu näiteks andmekirjete kronoloogiline järjestus, tuleks elektroonilisi arvestusraamatuid eristada muudest usaldusteenustest, nagu e-ajatemplid ja registreeritud e-andmevahetusteenused. Õiguskindluse tagamiseks ja innovatsiooni edendamiseks tuleks luua kogu liitu hõlmav õigusraamistik, mis näeb ette andmete kvalifitseeritud elektroonilistesse arvestusraamatutesse kandmiseks kasutatavate usaldusteenuste piiriülese tunnustamise. See peaks piisavalt suutma ära hoida, et sama digitaalset vara kopeeritakse ja müüakse eri isikutele rohkem kui üks kord. Elektroonilise arvestusraamatu loomise ja ajakohastamise protsess sõltub kasutatava arvestusraamatu liigist, nimelt sellest, kas tegemist on tsentraliseeritud või hajutatud arvestusraamatuga. Käesoleva määrusega tuleks tagada tehnoloogiline neutraalsus, nii et ei eelistata ega diskrimineerita mis tahes tehnoloogiat, mida kasutatakse elektrooniliste arvestusraamatute uue usaldusteenuse rakendamiseks. Lisaks peaks komisjon seoses kliimale avalduva kahjuliku mõjuga või muu kahjuliku keskkonnamõjuga võtma asjakohaste meetodite abil arvesse kestlikkusnäitajaid, kui ta valmistab ette rakendusakte, milles täpsustatakse kvalifitseeritud elektroonilistele arvestusraamatutele esitatavaid nõudeid.

(69) Elektroonilistele arvestusraamatutele usaldusteenuse osutajate ülesanne on teha kindlaks, et andmed kantakse arvestusraamatusse kronoloogilises järjestuses. Käesolev määrus ei piira elektrooniliste arvestusraamatute kasutajate liidu või riigisisesest õigusest tulenevaid õiguslikke kohustusi. Näiteks isikuandmete töötlemisega seotud kasutusjuhud peaksid olema kooskõlas määrusega (EL) 2016/679 ja finantsteenustega seotud kasutusjuhtumid peaksid olema kooskõlas asjaomase liidu finantsteenuste valdkonna õigusega.

(70) Et vältida siseturu killustatust ja tõkkeid, mis tulenevad standardite lahknevusest ja tehnilistest piirangutest, ning tagada koordineeritud protsess, et mitte mõjutada Euroopa digiidentiteedi raamistiku rakendamist, on vaja komisjoni, liikmesriikide, kodanikuühiskonna, akadeemiliste ringkondade ja erasektori tihedat ja struktureeritud koostööd. Selle eesmärgi saavutamiseks peaksid liikmesriigid ja komisjon tegema koostööd komisjoni soovituses (EL) 2021/946[16] sätestatud raamistikus, et määrata kindlaks ühised liidu tööriistad Euroopa digiidentiteedi raamistiku jaoks. Sellega seoses peaksid liikmesriigid leppima kokku põhjaliku tehnilise arhitektuuri ja võrdlusraamistiku, ühiste standardite ja tehniliste viidete kogumi, mis hõlmab olemasolevaid tunnustatud standardeid, ning juhiste ja heade tavade kirjelduste kogumi, mis peaks hõlmama vähemalt Euroopa digiidentiteedikukrute, sealhulgas e-allkirjade, ning elektrooniliste tõendite kvalifitseeritud usaldusteenuse osutajate kõiki funktsioone ja koostalitlusvõimet vastavalt käesolevas määruses sätestatule. Sellega seoses peaksid liikmesriigid samuti kokku leppima Euroopa digiidentiteedikukrute ärimudeli ja teenustasude struktuuri ühised elemendid, et hõlbustada nende kasutuselevõttu piiriülestes suhetes, eriti VKEde poolt. Tööriistad peaksid arenema paralleelselt Euroopa digiidentiteedi raamistiku üle peetava aruteluga ja raamistiku vastuvõtmise protsessiga ning kajastama nende tulemusi.

---

[16] Komisjoni 3. juuni 2021. aasta soovitus (EL) 2021/946, mis käsitleb ühiseid liidu tööriistu Euroopa digiidentiteedi raamistiku koordineeritud käsitlusviisi jaoks (ELT L 210, 14.6.2021, lk 51).

(71) Käesolevas määruses sätestatakse kvalifitseeritud usaldusteenuste kvaliteedi, usaldusväärsuse ja turvalisuse ühtlustatud tase, olenemata sellest, kus neid toiminguid tehakse. Seega peaks kvalifitseeritud usaldusteenuse osutajal olema lubatud anda kvalifitseeritud usaldusteenuse osutamisega seotud toimingud edasi kolmandasse riiki, kui kõnealune kolmas riik esitab piisavad tagatised, millega kindlustatakse, et järelevalvetegevuse ja auditite läbiviimist saab tagada nii, nagu need oleksid tehtud liidus. Kui käesoleva määruse järgimist ei ole võimalik täielikult tagada, peaks järelevalveasutustel olema võimalik võtta proportsionaalseid ja põhjendatud meetmeid, sealhulgas osutatavalt usaldusteenuselt kvalifitseeritud staatuse äravõtmine.

(72) Selleks et tagada õiguskindlus seoses kvalifitseeritud sertifikaatidel põhinevate täiustatud e-allkirjade kehtivusega, on väga oluline täpsustada, millise hinnangu annab tuginev isik, kes valideerib kõnealuse kvalifitseeritud sertifikaatidel põhineva täiustatud e-allkirja.

(73) Usaldusteenuse osutajad peaksid kasutama krüptomeetodeid, mis kajastavad praegusi parimaid tavasid ja nende algoritmide usaldusväärset rakendamist, et tagada oma usaldusteenuste turvalisus ja usaldusväärsus.

(74) Käesolevas määruses sätestatakse kvalifitseeritud usaldusteenuse osutajate kohustus kontrollida selliste füüsiliste või juriidiliste isikute identiteeti, kellele kvalifitseeritud sertifikaat või kvalifitseeritud elektrooniline tõend on väljastatud, kasutades erinevaid liidus ühtlustatud meetodeid. Tagamaks, et kvalifitseeritud sertifikaadid ja kvalifitseeritud elektroonilised tõendid väljastatakse isikule, kellele need kuuluvad, ning et need tõendavad õiget ja kordumatut andmekogumit, mis näitab selle isiku identiteeti, peaksid kvalifitseeritud sertifikaate või kvalifitseeritud elektroonilisi tõendeid väljastavad kvalifitseeritud usaldusteenuse osutajad kõnealuste sertifikaatide ja tõendite väljastamise ajal tagama selle isiku identimise täie kindlusega. Lisaks isiku identiteedi kohustuslikule kontrollimisele, kui see on kohaldatav kvalifitseeritud sertifikaatide ja kvalifitseeritud elektrooniliste tõendite väljastamiseks, peaksid kvalifitseeritud usaldusteenuse osutajad tagama täie kindlusega selle isiku tõendatud atribuutide õigsuse ja täpsuse, kellele kvalifitseeritud sertifikaat või kvalifitseeritud elektrooniline tõend on väljastatud. Kõnealuseid tulemuse saavutamise ja täieliku kindlusega seotud kohustusi tõendatud andmete kontrollimisel tuleks toetada asjakohaste vahenditega, sealhulgas kasutades käesolevas määruses ette nähtud erimeetodit või vajaduse korral mitme erimeetodi kombinatsiooni. Neid meetodeid peaks olema võimalik kombineerida, et luua sobiv alus selle isiku identiteedi kontrollimiseks, kellele kvalifitseeritud sertifikaat või kvalifitseeritud elektrooniline tõend väljastatakse. Selline kombinatsioon peaks hõlmama tuginemist e-identimise vahenditele, mis vastavad märkimisväärse usaldusväärsuse taseme nõuetele koos muude identiteedi kontrollimise vahenditega. E-identimine võimaldaks täita käesolevas määruses sätestatud kõrge usaldusväärsuse tasemega seotud ühtlustatud nõudeid sellise täiendava ühtlustatud kaugmenetluse osana, tagades identimise kõrgel usaldusväärsuse tasemel. Need meetodid peaksid hõlmama võimalust, et kvalifitseeritud elektroonilist tõendit väljastav kvalifitseeritud usaldusteenuse osutaja saaks kasutaja taotlusel, kooskõlas liidu või riigisisese õigusega kontrollida elektrooniliselt tõendatavaid atribuute, sealhulgas autentsete allikate põhjal.

(75) Et tagada käesoleva määruse kooskõla üleilmsete arengusuundumustega ja järgida siseturu parimaid tavasid, tuleks komisjoni vastu võetud delegeeritud õigusaktid ja rakendusaktid korrapäraselt läbi vaadata ja vajaduse korral tuleks neid ajakohastada. Ajakohastamise vajalikkuse hindamisel tuleks arvesse võtta uusi tehnoloogiaid, tavasid, standardeid või tehnilisi kirjeldusi.

(76) Kuna käesoleva määruse eesmärke, milleks on töötada välja kogu liitu hõlmav Euroopa digiidentiteedi raamistik ja usaldusteenuse raamistik, ei suuda liikmesriigid piisavalt saavutada, küll aga saab neid meetme ulatuse ja toime tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärkide saavutamiseks vajalikust kaugemale.

(77) Euroopa Andmekaitseinspektoriga konsulteeriti kooskõlas määruse (EL) 2018/1725 artikli 42 lõikega 1.

(78) Määrust (EL) nr 910/2014 tuleks seetõttu vastavalt muuta,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Määruse (EL) nr 910/2014 muutmine

Määrust (EL) nr 910/2014 muudetakse järgmiselt.

1) Artikkel 1 asendatakse järgmisega:

„*Artikkel 1*

Reguleerimisese

Käesoleva määruse eesmärk on tagada siseturu nõuetekohane toimimine ning kogu liidus kasutatavate e-identimise vahendite ja usaldusteenuste asjakohane turvalisuse tase, et võimaldada füüsilistel ja juriidilistel isikutel kasutada õigust osaleda turvaliselt digiühiskonnas ning pääseda juurde internetipõhistele avalikele ja erasektori teenustele kogu liidus ning hõlbustada neil selle õiguse kasutamist. Neil eesmärkidel käesolevas määruses:

a) sätestatakse tingimused, mille alusel liikmesriigid tunnustavad füüsiliste ja juriidiliste isikute e-identimise vahendeid, mis kuuluvad teise liikmesriigi teavitatud e-identimise süsteemi, ning teevad kättesaadavaks ja tunnustavad Euroopa digiidentiteedikukruid;

b) sätestatakse normid usaldusteenuste, eelkõige e-tehingute jaoks;

c) luuakse õigusraamistik e-allkirja, e-templi, e-ajatempli, e-dokumentide, registreeritud e-andmevahetusteenuste, veebisaitide autentimise sertifitseerimisteenuste, elektroonilise arhiveerimise, elektrooniliste tõendite, e-allkirja andmise vahendite, e-templi loomise vahendite ning elektrooniliste arvestusraamatute jaoks.“

2) Artiklit 2 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Käesolevat määrust kohaldatakse liikmesriigi poolt teavitatud e-identimise süsteemide, liikmesriigi poolt kättesaadavaks tehtud Euroopa digiidentiteedikukrute ja liidus asutatud usaldusteenuse osutajate suhtes.“;

b) lõige 3 asendatakse järgmisega:

„3. Käesolev määrus ei mõjuta liidu või riigisisest õigust, mis reguleerib lepingute sõlmimist ja kehtivust, muid õiguslikke või menetluslikke kohustusi seoses vormiga ega sektoripõhiseid vorminõudeid.

4. Käesolev määrus ei piira Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679* kohaldamist.

---

* Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).“

3) Artiklit 3 muudetakse järgmiselt.

a) Punktid 1–5 asendatakse järgmisega:

„1) „e-identimine“ – protsess, mille käigus kasutatakse elektroonilisi isikutuvastusandmeid, mis tähistavad üheselt füüsilist või juriidilist isikut või teist füüsilist isikut või juriidilist isikut esindavat füüsilist isikut;

2) „e-identimise vahend“ – kehaline ja/või kehatu üksus, mis sisaldab isikutuvastusandmeid ja mida kasutatakse autentimiseks internetipõhiste või asjakohasel juhul veebiväliste teenuste puhul;

3) „isikutuvastusandmed“ – liidu või riigisisese õiguse kohaselt väljastatud andmed, mis võimaldavad teha kindlaks füüsilise või juriidilise isiku või teist füüsilist isikut või juriidilist isikut esindava füüsilise isiku;

4) „e-identimise süsteem“ – e-identimiseks vajalik süsteem, mille raames väljastatakse e-identimise vahendeid füüsilistele või juriidilistele isikutele või teist füüsilist isikut või juriidilist isikut esindavatele füüsilistele isikutele;

5) „autentimine“ – elektrooniline protsess, mis võimaldab füüsilise või juriidilise isiku e-identimise kinnitamist või elektrooniliste andmete päritolu ja tervikluse kinnitamist;“;

b) lisatakse järgmine punkt:

„5a) „kasutaja“ – füüsiline või juriidiline isik või teist füüsilist isikut või juriidilist isikut esindav füüsiline isik, kes kasutab käesoleva määruse kohaselt pakutavaid usaldusteenuseid või e-identimise vahendeid;“;

c) punkt 6 asendatakse järgmisega:

„6) „tuginev isik“ – füüsiline või juriidiline isik, kes tugineb e-identimisele, Euroopa digiidentiteedikukrutele või muudele e-identimise vahenditele või usaldusteenusele;“;

d) punkt 16 asendatakse järgmisega:

„16) „usaldusteenus“ – elektrooniline teenus, mida tavaliselt osutatakse tasu eest ja mis hõlmab üht järgmistest:

a) e-allkirja sertifikaatide, e-templi sertifikaatide, veebisaidi autentimise sertifikaatide või muude usaldusteenuste osutamiseks vajalike sertifikaatide väljastamine;

b) e-allkirja sertifikaatide, e-templi sertifikaatide, veebisaidi autentimise sertifikaatide või muude usaldusteenuste osutamiseks vajalike sertifikaatide valideerimine;

c) e-allkirjade või e-templite loomine;

d) e-allkirjade või e-templite valideerimine;

e) e-allkirjade, e-templite, e-allkirja sertifikaatide või e-templi sertifikaatide säilitamine;

f) e-allkirja või e-templi kaugloomise vahendite haldamine;

g) elektrooniliste tõendite väljastamine;

h) elektrooniliste tõendite valideerimine;

i) e-ajatemplite loomine;

j) e-ajatemplite valideerimine;

k) registreeritud e-andmevahetusteenuste osutamine;

l) registreeritud e-andmevahetusteenuste kaudu edastatud andmete ja nendega seotud tõendite valideerimine;

m) elektrooniliste andmete ja e-dokumentide elektrooniline arhiveerimine;

n) elektrooniliste andmete kandmine elektroonilisse arvestusraamatusse;“;

e) punkt 18 asendatakse järgmisega:

„18) „vastavushindamisasutus“ – määruse (EÜ) nr 765/2008 artikli 2 punktis 13 määratletud vastavushindamisasutus, mis on kooskõlas nimetatud määrusega akrediteeritud kui asutus, mis on pädev tegema kvalifitseeritud usaldusteenuse osutaja ja tema osutatavate kvalifitseeritud usaldusteenuste vastavushindamist või on pädev sertifitseerima Euroopa digiidentiteedikukruid või e-identimise vahendeid;“;

f) punkt 21 asendatakse järgmisega:

„21) „toode“ – riist- või tarkvara või riist- või tarkvara asjakohased osad, mis on ette nähtud e-identimiseks ja usaldusteenuste osutamiseks;“;

g) lisatakse järgmised punktid:

„23a) „kvalifitseeritud e-allkirja kaugloomise vahend“ – kvalifitseeritud e-allkirja andmise vahend, mida kvalifitseeritud usaldusteenuse osutaja haldab allkirja andja nimel vastavalt artiklile 29a;

23b) „kvalifitseeritud e-templi kaugloomise vahend“ – kvalifitseeritud e-templi loomise vahend, mida kvalifitseeritud usaldusteenuse osutaja haldab templi looja nimel vastavalt artiklile 39a; “;

h) punkt 38 asendatakse järgmisega:

„38) „veebisaidi autentimise sertifikaat“ – elektrooniline tõend, mis võimaldab autentida veebisaiti ja seob selle füüsilise või juriidilise isikuga, kellele sertifikaat on väljastatud;“;

i) punkt 41 asendatakse järgmisega:

„41) „valideerimine“ – protsess, mille käigus kontrollitakse ja kinnitatakse, et elektroonilised andmed on käesoleva määruse kohaselt kehtivad;“;

j) lisatakse järgmised punktid:

„42) „Euroopa digiidentiteedikukkur“ – e-identimise vahend, mis võimaldab kasutajal turvaliselt salvestada, hallata ja valideerida isikutuvastusandmeid ja elektroonilisi tõendeid, et esitada neid tuginevatele isikutele ja teistele Euroopa digiidentiteedikukrute kasutajatele, ning allkirjastada kvalifitseeritud e-allkirjaga või kinnitada kvalifitseeritud e-templiga;

43) „atribuut“ – füüsilise või juriidilise isiku või eseme tunnus, omadus, õigus või luba;

44) „elektrooniline tõend“ – elektrooniline tõend, mis võimaldab atribuute autentida;

45) „kvalifitseeritud elektrooniline tõend“ – elektrooniline tõend, mille on väljastanud kvalifitseeritud usaldusteenuse osutaja ja mis vastab V lisas sätestatud nõuetele;

46) „autentse allika eest vastutava avaliku sektori asutuse või tema nimel välja antud elektrooniline tõend“ – elektrooniline tõend, mille on välja andnud autentse allika eest vastutav avaliku sektori asutus või avaliku sektori asutus, kelle liikmesriik on määranud välja andma selliseid tõendeid autentsete allikate eest vastutavate avaliku sektori asutuste nimel kooskõlas artikliga 45f ja VII lisaga;

47) „autentne allikas“ – avaliku sektori asutuse või eraõigusliku isiku vastutusel olev andmehoidla või süsteem, mis sisaldab ja pakub füüsilise või juriidilise isiku või eseme atribuute ja mida peetakse selle teabe peamiseks allikaks või mis on liidu või riigisisese õiguse, sealhulgas haldustava kohaselt tunnustatud autentsena;

48) „elektrooniline arhiveerimine“ – teenus, millega tagatakse elektrooniliste andmete ja e-dokumentide vastuvõtmine, säilitamine, otsimine ja kustutamine, et tagada nende säilivus ja loetavus ning säilitada nende terviklus, konfidentsiaalsus ja päritolutõend kogu säilitamisaja jooksul;

49) „kvalifitseeritud elektroonilise arhiveerimise teenus“ – elektroonilise arhiveerimise teenus, mida osutab kvalifitseeritud usaldusteenuse osutaja ja mis vastab artiklis 45j sätestatud nõuetele;

50) „ELi digiidentiteedikukru usaldusmärk“ – selgelt esitatud kontrollitav, lihtne ja äratuntav märge selle kohta, et Euroopa digiidentiteedikukrut pakutakse kooskõlas käesoleva määrusega;

51) „tugev kasutaja autentimine“ – autentimine, mille käigus kasutatakse vähemalt kahte erineva kategooria autentimistegurit, mis kuuluvad teadmise (miski, mida teab üksnes kasutaja), valdamise (miski, mida valdab üksnes kasutaja) või tunnuse (miski, mis on kasutajale omane) kategooriasse ja on sõltumatud, nii et turvarikkumine neist ühe puhul ei kahjustaks teiste usaldusväärsust, ning mille ülesehitus võimaldab kaitsta autentimisandmete konfidentsiaalsust;

52) „elektrooniline arvestusraamat“ – elektrooniliste andmekirjete jada, mis tagab nende kirjete tervikluse ja nende kirjete kronoloogilise järjestuse täpsuse;

53) „kvalifitseeritud elektrooniline arvestusraamat“ – elektrooniline arvestusraamat, mille teeb kättesaadavaks kvalifitseeritud usaldusteenuse osutaja ja mis vastab artiklis 45l sätestatud nõuetele;

54) „isikuandmed“ – igasugune määruse (EL) 2016/679 artikli 4 punktis 1 määratletud teave;

55) „identiteedi ühitamine“ – protsess, mille käigus isikutuvastusandmed või e-identimise vahendid ühendatakse või seotakse samale isikule kuuluva olemasoleva kontoga;

56) „andmekirje“ – elektroonilised andmed, mis on salvestatud koos seotud metaandmetega, mis toetavad andmete töötlemist;

57) „võrguväline“ – Euroopa digiidentiteedikukrute puhul kasutaja ja kolmanda isiku vaheline suhtlus füüsilises asukohas, kasutades lähisidetehnoloogiat, mille puhul ei ole digiidentiteedikukrul vaja suhtluse eesmärgil elektroonilise side võrkude kaudu kaugsüsteemidele juurde pääseda.“

4) Artikkel 5 asendatakse järgmisega:

„*Artikkel 5*
Varjunimed e-tehingute tegemisel

Ilma et see piiraks kasutajate suhtes kohaldatavate endi identimise nõuet käsitlevate liidu või riigisisese õiguse kohaste erinormide kohaldamist või riigisisese õiguse kohast varjunimede õiguslikku toimet, ei keelata e-tehingute tegemisel kasutaja valitud varjunimede kasutamist. “

5) II peatükki lisatakse järgmine jagu:

„1. JAGU
EUROOPA DIGIIDENTITEEDIKUKKUR

Artikkel 5a
Euroopa digiidentiteedikukrud

1. Tagamaks, et kõigil liidu füüsilistel ja juriidilistel isikutel on turvaline, usaldusväärne ja sujuv piiriülene juurdepääs avalikele ja erasektori teenustele, omades seejuures täielikku kontrolli oma andmete üle, teeb iga liikmesriik 24 kuu jooksul käesoleva artikli lõikes 23 ja artikli 5c lõikes 6 osutatud rakendusaktide jõustumise kuupäevast kättesaadavaks vähemalt ühe Euroopa digiidentiteedikukru.

2. Euroopa digiidentiteedikukkur tehakse kättesaadavaks ühel või mitmel järgmisel viisil:

   a) vahetult liikmesriigi poolt;

   b) liikmesriigi antud volituse alusel;

   c) liikmesriigist sõltumatult, kuid liikmesriik tunnustab seda.

3. Euroopa digiidentiteedikukrute rakendustarkvara komponentide lähtekood on avatud lähtekood. Liikmesriigid võivad ette näha, et igakülgselt põhjendatud juhtudel ei avalikustata muude kui kasutajaseadmetele paigaldatud konkreetsete komponentide lähtekoodi.

4. Euroopa digiidentiteedikukrud võimaldavad kasutajal kasutajasõbralikul, läbipaistval ja kasutaja poolt jälgitaval viisil

a) turvaliselt taotleda, saada, valida, kombineerida, salvestada, kustutada, jagada ja esitada kasutaja ainukontrolli all isikutuvastusandmeid, ning kui see on kohaldatav, koos elektrooniliste tõenditega autentida tuginevate isikute jaoks võrgus ja asjakohasel juhul võrguväliselt, et pääseda juurde avalikele ja erasektori teenustele, tagades samal ajal andmete valikulise avaldamise võimaluse;

b) luua varjunimesid ja salvestada need krüpteerituna ja lokaalselt Euroopa digiidentiteedikukrus;

c) turvaliselt autentida teise isiku Euroopa digiidentiteedikukrut ning saada ja vahetada isikutuvastusandmeid ja elektroonilisi tõendeid turvalisel viisil kahe Euroopa digiidentiteedikukru vahel;

d) saada juurdepääsu kõigi Euroopa digiidentiteedikukru kaudu tehtud tehingute logile ühise töölaua kaudu, mis võimaldab kasutajal

i) vaadata ajakohastatud selliste tuginevate isikute loetelu, kellega kasutaja on loonud ühenduse, ja kui see on kohaldatav, kõiki vahetatud andmeid;

ii) taotleda tuginevalt isikult hõlpsasti isikuandmete kustutamist vastavalt määruse (EL) 2016/679 artiklile 17;

iii) teatada hõlpsasti tuginevast isikust pädevale riiklikule andmekaitseasutusele, kui on saadud väidetavalt ebaseaduslik või kahtlane taotlus andmete saamiseks;

e) allkirjastada kvalifitseeritud e-allkirjaga või kinnitada kvalifitseeritud e-tempiga;

f) laadida alla kasutaja andmeid, elektroonilisi tõendeid ja konfiguratsioone tehniliselt mõistlikus ulatuses;

g) kasutada kasutaja õigust andmete ülekantavusele.

5. Euroopa digiidentiteedikukrud peavad eelkõige

a) toetama ühiseid protokolle ja liideseid, et

i) väljastada Euroopa digiidentiteedikukrule isikutuvastusandmeid, kvalifitseeritud ja kvalifitseerimata elektroonilisi tõendeid või kvalifitseeritud ja kvalifitseerimata sertifikaate;

ii) tuginevatel isikutel oleks võimalik taotleda ja valideerida isikutuvastusandmeid ja elektroonilisi tõendeid;

iii) jagada ja esitada tuginevatele isikutele võrgus ja asjakohasel juhul võrguväliselt isikutuvastusandmeid, elektroonilisi tõendeid või valikuliselt avaldatud seotud andmeid;

iv) kasutajal oleks võimalik suhelda Euroopa digiidentiteedikukruga ja kuvada ELi digiidentiteedikukru usaldusmärki;

v) kasutaja turvaliselt aktiveerida, kasutades artikli 5a lõike 24 kohast e-identimise vahendit;

vi) suhelda kahe isiku Euroopa digiidentiteedikukruga eesmärgiga saada, vahetada ja valideerida isikutuvastusandmeid ja elektroonilisi tõendeid turvalisel viisil;

vii) autentida ja identifitseerida tuginevaid isikuid, rakendades autentimismehhanisme kooskõlas artikliga 5b;

viii) tuginevad isikud saaksid kontrollida Euroopa digiidentiteedikukru autentsust ja kehtivust;

ix) tuginevalt isikult saaks taotleda isikuandmete kustutamist vastavalt määruse (EL) 2016/679 artiklile 17;

x) tuginevast isikust saaks teatada pädevale riiklikule andmekaitseasutusele, kui on saadud väidetavalt ebaseaduslik või kahtlane taotlus andmete saamiseks;

xi) võimaldada luua kvalifitseeritud e-allkirju või e-templeid kvalifitseeritud e-allkirja andmise või e-templi loomise vahendite abil;

b) mitte andma elektrooniliste tõendite usaldusteenuste osutajatele mingit teavet nende elektrooniliste tõendite kasutamise kohta;

c) tagama, et tuginevaid isikuid saab autentida ja identifitseerida, rakendades autentimismehhanisme kooskõlas artikliga 5b;

d) vastama artiklis 8 sätestatud nõuetele kõrge usaldusväärsuse taseme kohta, eelkõige seoses identiteedi tõendamise ja kontrollimise ning e-identimise vahendite haldamise ja autentimise nõuetega;

e) rakendama integreeritud avalikustamispoliitikaga elektrooniliste tõendite korral asjakohast mehhanismi, et teavitada kasutajat sellest, et tugineval isikul või kõnealust elektroonilist tõendit taotleval Euroopa digiidentiteedikukru kasutajal on tõendile juurdepääsuks luba;

f) tagama, et isikutuvastusandmed, mis on kättesaadavad e-identimise süsteemi kaudu, mille alusel Euroopa digiidentiteedikukrut pakutakse, tähistavad üheselt füüsilist isikut, juriidilist isikut või füüsilist või juriidilist isikut esindavat füüsilist isikut ning on seotud selle Euroopa digiidentiteedikukruga;

g) pakkuma kõigile füüsilistele isikutele vaikimisi ja tasuta võimalust anda allkiri kvalifitseeritud e-allkirjana.

Olenemata esimese lõigu punktist g võivad liikmesriigid ette näha proportsionaalsed meetmed tagamaks, et kvalifitseeritud e-allkirjade tasuta kasutamine füüsiliste isikute poolt piirdub mittekutseliste eesmärkidega.

6. Liikmesriigid teavitavad viivitamata kasutajaid igast turvarikkumisest, mis võis täielikult või osaliselt kahjustada nende Euroopa digiidentiteedikukrut või selle sisu, ning eelkõige juhul, kui nende Euroopa digiidentiteedikukru kehtivus on artikli 5e kohaselt peatatud või see on kehtetuks tunnistatud.

7. Ilma et see piiraks artikli 5f kohaldamist, võivad liikmesriigid kooskõlas riigisisese õigusega näha ette Euroopa digiidentiteedikukrute lisafunktsioonid, sealhulgas koostalitlusvõime olemasolevate riiklike e-identimise vahenditega. Need lisafunktsioonid peavad vastama käesolevale artiklile.

8. Liikmesriigid pakuvad tasuta valideerimismehhanisme, et

   a) Euroopa digiidentiteedikukrute autentsust ja kehtivust saab kontrollida;

   b) võimaldada kasutajatel kontrollida artikli 5b kohaselt registreeritud tuginevate isikute identiteedi autentsust ja kehtivust.

9. Liikmesriigid tagavad, et Euroopa digiidentiteedikukru saab kehtetuks tunnistada järgmistel juhtudel:

   a) kasutaja sõnaselge taotluse korral;

   b) kui Euroopa digiidentiteedikukru turvalisust on kahjustatud;

   c) kasutaja surma või juriidilise isiku tegevuse lõppemise korral.

10. Euroopa digiidentiteedikukrute pakkujad tagavad, et kasutajad saavad hõlpsasti taotleda tehnilist tuge ja teatada tehnilistest probleemidest või muudest intsidentidest, millel on negatiivne mõju Euroopa digiidentiteedikukru kasutamisele.

11. Euroopa digiidentiteedikukruid pakutakse kõrge usaldusväärsuse tasemega e-identimise süsteemi alusel.

12. Euroopa digiidentiteedikukrul on lõimitud turve.

13. Euroopa digiidentiteedikukrud väljastatakse, neid kasutatakse ja need tunnistatakse kõigi füüsiliste isikute jaoks kehtetuks tasuta.

14. Kasutajatel on täielik kontroll oma Euroopa digiidentiteedikukru kasutamise ja selles sisalduvate andmete üle. Euroopa digiidentiteedikukru pakkuja ei kogu Euroopa digiidentiteedikukru kasutamise kohta teavet, mida ei ole vaja Euroopa digiidentiteedikukru teenuste osutamiseks, ega kombineeri isikutuvastusandmeid või muid salvestatud või Euroopa digiidentiteedikukru kasutamisega seotud isikuandmeid selliste isikuandmetega, mis pärinevad selle pakkuja pakutavatest muudest teenustest või kolmandate isikute pakutavatest teenustest ja mida ei ole vaja Euroopa digiidentiteedikukru teenuste osutamiseks, välja arvatud juhul, kui kasutaja on sõnaselgelt teisiti taotlenud. Euroopa digiidentiteedikukrute pakkumisega seotud isikuandmeid hoitakse loogiliselt lahus kõigist muudest Euroopa digiidentiteedikukru pakkuja valduses olevatest andmetest. Kui Euroopa digiidentiteedikukrut pakub eraõiguslik isik vastavalt käesoleva artikli lõike 2 punktidele b ja c, kohaldatakse artikli 45h lõiget 3 *mutatis mutandis*.

15. Euroopa digiidentiteedikukrute kasutamine on vabatahtlik. Euroopa digiidentiteedikukruid mittekasutavate füüsiliste või juriidiliste isikute juurdepääsu avalikele ja erasektori teenustele ja tööturule ning ettevõtlusvabadust ei tohi mingil moel piirata ega takistada. Avalikele ja erasektori teenustele juurdepääs peab olema jätkuvalt võimalik ka muude olemasolevate identimis- ja autentimisvahendite abil.

16. Euroopa digiidentiteedikukru tehniline raamistik

    a) ei tohi võimaldada elektrooniliste tõendite pakkujatel ega muudel isikutel pärast atribuutide tõendamist saada andmeid, mis võimaldavad tehinguid või kasutaja käitumist jälgida, seostada, korreleerida või saada muul viisil teavet tehingute või kasutaja käitumise kohta, välja arvatud juhul, kui kasutaja on selleks sõnaselge loa andnud;

    b) võimaldab privaatsuse säilitamise viise, mis tagavad seostamatuse, kui atribuutide tõendamine ei nõua kasutaja identimist.

17. Isikuandmete töötlemine liikmesriigi poolt või liikmesriigi nimel selliste asutuste või isikute poolt, kes vastutavad Euroopa digiidentiteedikukrute e-identimise vahendina pakkumise eest, toimub kooskõlas asjakohaste ja mõjusate andmekaitsemeetmetega. Sellise töötlemise vastavust määrusele (EL) 2016/679 tuleb tõendada. Liikmesriigid võivad kehtestada riigisiseseid sätteid, et täpsustada selliste meetmete kohaldamist.

18. Liikmesriigid edastavad komisjonile põhjendamatu viivituseta järgmise teabe:

a) asutus, kes vastutab Euroopa digiidentiteedikukrutele tuginevate registreeritud tuginevate isikute loetelu koostamise ja haldamise eest vastavalt artikli 5b lõikele 5, ja selle loetelu asukoht;

b) asutused, kes vastutavad Euroopa digiidentiteedikukrute pakkumise eest vastavalt artikli 5a lõikele 1;

c) asutused, kes vastutavad selle tagamise eest, et isikutuvastusandmed on seotud Euroopa digiidentiteedikukruga vastavalt artikli 5a lõike 5 punktile f;

d) mehhanism, mis võimaldab artikli 5a lõike 5 punktis f osutatud isikutuvastusandmeid ja tuginevate isikute identiteeti valideerida;

e) Euroopa digiidentiteedikukru autentsuse ja kehtivuse valideerimise mehhanism.

Komisjon teeb esimese lõigu kohaselt edastatud teabe turvalise kanali kaudu üldsusele kättesaadavaks elektrooniliselt allkirjastatud või e-templiga varustatud formaadis, mis sobib automaatseks töötlemiseks.

19. Artiklit 11 kohaldatakse *mutatis mutandis* Euroopa digiidentiteedikukru suhtes, piiramata käesoleva artikli lõike 22 kohaldamist.

20. Artikli 24 lõike 2 punkte b ning d–h kohaldatakse *mutatis mutandis* Euroopa digiidentiteedikukrute pakkujate suhtes.

21. Euroopa digiidentiteedikukrud tehakse puuetega inimestele kasutamiseks ligipääsetavaks teiste kasutajatega võrdsetel alustel kooskõlas Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2019/882*.

22. Euroopa digiidentiteedikukrute pakkumise eesmärgil ei kohaldata Euroopa digiidentiteedikukrute ja e-identimise süsteemide suhtes, mille raames neid pakutakse, artiklites 7, 9, 10, 12 ja 12a sätestatud nõudeid.

23. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõigetes 4, 5, 8 ja 18 osutatud nõuete jaoks, mis käsitlevad Euroopa digiidentiteedikukru rakendamist. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

24. Komisjon kehtestab rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused, et hõlbustada Euroopa digiidentiteedikukru kasutajate jaoks aktiveerimist, kasutades kas kõrgele usaldusväärsuse tasemele vastavaid e-identimise vahendeid või märkimisväärsele usaldusväärsuse tasemele vastavaid e-identimise vahendeid koos täiendavate kaugaktiveerimismenetlustega, mis üheskoos vastavad kõrge usaldusväärsuse taseme nõuetele. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 5b

Euroopa digiidentiteedikukrule tuginevad isikud

1. Kui tuginev isik kavatseb tugineda Euroopa digiidentiteedikukrutele, et osutada avalikke või erateenuseid digitaalse suhtluse kaudu, registreerib tuginev isik end liikmesriigis, kus ta on asutatud.

2. Registreerimisprotsess peab olema kulutõhus ja riski suhtes proportsionaalne. Tuginev isik esitab vähemalt järgmise teabe:

   a) teave, mida on vaja autentimiseks Euroopa digiidentiteedikukrute jaoks, mis hõlmab vähemalt järgmist:

      i) liikmesriik, kus tuginev isik on asutatud, ning

      ii) tugineva isiku nimi ja kui see on olemas, siis tema ametlikus registris esitatud registreerimisnumber koos selle ametliku registri identimisandmetega;

b) tugineva isiku kontaktandmed;

c) Euroopa digiidentiteedikukrute kavandatud kasutus, sealhulgas viide andmetele, mida tuginev isik kasutajatelt taotleb.

3. Tuginevad isikud ei taotle kasutajatelt muude andmete esitamist kui need, millele on osutatud lõike 2 punktis c.

4. Lõiked 1 ja 2 ei piira liidu ega riigisisest õigust, mida kohaldatakse konkreetsete teenuste osutamise suhtes.

5. Liikmesriigid teevad lõikes 2 osutatud teabe veebis üldsusele kättesaadavaks elektrooniliselt allkirjastatud või e-templiga varustatud formaadis, mis sobib automaatseks töötlemiseks.

6. Käesoleva artikli kohaselt registreeritud tuginevad isikud teavitavad liikmesriike viivitamata lõike 2 kohaselt registreerimisel esitatud teabe muutumisest.

7. Liikmesriigid kehtestavad ühise mehhanismi, mis võimaldab tuginevad isikud identida ja autentida, nagu on osutatud artikli 5a lõike 5 punktis c.

8. Kui tuginevad isikud kavatsevad tugineda Euroopa digiidentiteedikukrutele, idendivad nad end kasutajale.

9. Tuginevad isikud vastutavad Euroopa digiidentiteedikukrutest taotletavate isikutuvastusandmete ja elektrooniliste tõendite autentimise ja valideerimise menetluse läbiviimise eest. Tuginevad isikud ei tohi olla vastu varjunimede kasutamisele, kui kasutaja identimine ei ole liidu või liikmesriigi õiguse kohaselt nõutav.

10. Tuginevate isikute nimel tegutsevaid vahendajaid käsitatakse tuginevate isikutena ja nad ei tohi salvestada andmeid tehingu sisu kohta.

11. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon käesoleva artikli lõigetes 2, 5 ja 6–9 osutatud nõuete jaoks tehnilised kirjeldused ja menetlused artikli 5a lõikes 23 osutatud rakendusaktidega, mis käsitlevad Euroopa digiidentiteedikukrute rakendamist. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 5c

Euroopa digiidentiteedikukrute sertifitseerimine

1. Liikmesriikide määratud vastavushindamisasutused sertifitseerivad Euroopa digiidentiteedikukrute ja e-identimise süsteemi, mille alusel neid pakutakse, vastavuse artikli 5a lõigetes 4, 5 ja 8 sätestatud nõuetele, artikli 5a lõikes 14 sätestatud loogiliselt lahus hoidmise nõudele, ning kui see on kohaldatav, artikli 5a lõikes 24 osutatud standarditele ja tehnilistele kirjeldustele.

2. Euroopa digiidentiteedikukrute või nende osade vastavuskäesoleva artikli lõikes 1 osutatud nõuetele, mis puudutavad küberturvalisust, sertifitseeritakse kooskõlas Euroopa küberturvalisuse sertifitseerimise kavadega, mis on vastu võetud Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881** kohaselt ja millele viidatakse käesoleva artikli lõikes 6 osutatud rakendusaktides.

3. Käesoleva artikli lõikes 1 osutatud nõuete puhul, mis ei puuduta küberturvalisust, ja käesoleva artikli lõikes 1 osutatud nõuete puhul, mis puudutavad küberturvalisust, niivõrd kui käesoleva artikli lõikes 2 osutatud küberturvalisuse sertifitseerimise kavad ei hõlma või hõlmavad üksnes osaliselt asjakohaseid küberturvalisuse nõudeid seoses nimetatud nõuetega, kehtestavad liikmesriigid riiklikud sertifitseerimiskavad, järgides käesoleva artikli lõikes 6 osutatud rakendusaktides sätestatud nõudeid. Liikmesriigid edastavad oma riiklike sertifitseerimiskavade kavandid artikli 46e lõike 1 kohaselt loodud Euroopa digiidentiteedi koostöörühmale (edaspidi „koostöörühm“). Koostöörühm võib esitada arvamusi ja soovitusi.

4. Lõike 1 kohane sertifitseerimine kehtib kuni viis aastat, tingimusel et iga kahe aasta järel viiakse läbi nõrkuste hindamine. Kui tehakse kindlaks nõrkus ja seda ei kõrvaldata õigeks ajaks, sertifitseerimine tühistatakse.

5. Isikuandmete töötlemise toimingutega seotud käesoleva määruse artiklis 5a sätestatud nõuete täitmist võib tõendada määruse (EL) 2016/679 kohaselt.

6. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõigetes 1, 2 ja 3 osutatud Euroopa digiidentiteedikukrute sertifitseerimise jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

7. Liikmesriigid teatavad komisjonile lõikes 1 osutatud vastavushindamisasutuste nimed ja aadressid. Komisjon teeb selle teabe kõigile liikmesriikidele kättesaadavaks.

8. Komisjonil on õigus võtta kooskõlas artikliga 47 vastu delegeeritud õigusakte, millega kehtestatakse konkreetsed kriteeriumid, millele käesoleva artikli lõikes 1 osutatud vastavushindamisasutused peavad vastama.

Artikkel 5d

Sertifitseeritud Euroopa digiidentiteedikukrute loetelu avaldamine

1. Liikmesriigid teatavad komisjonile ja artikli 46e lõike 1 kohaselt loodud koostöörühmale põhjendamatu viivituseta Euroopa digiidentiteedikukrutest, mis on tehtud kättesaadavaks artikli 5a kohaselt ja mille on sertifitseerinud artikli 5c lõikes 1 osutatud vastavushindamisasutused. Nad teavitavad komisjoni ja artikli 46e lõike 1 kohaselt loodud koostöörühma põhjendamatu viivituseta sertifitseerimise tühistamisest ja esitavad tühistamise põhjused.

2. Piiramata artikli 5a lõike 18 kohaldamist, sisaldab käesoleva artikli lõikes 1 osutatud liikmesriikide esitatav teave vähemalt järgmist:

   a) sertifitseeritud Euroopa digiidentiteedikukru sertifikaat ja sertifitseerimise hindamisaruanne;

   b) selle e-identimise süsteemi kirjeldus, mille alusel Euroopa digiidentiteedikukrut pakutakse;

   c) kohaldatav järelevalvekord ja Euroopa digiidentiteedikukru pakkuja vastutuskorda puudutav teave;

   d) e-identimise süsteemi eest vastutav asutus või vastutavad asutused;

   e) teavitatud e-identimise süsteemi, autentimise või asjaomase osa, mille turvalisust on kahjustatud, peatamise või kehtetuks tunnistamise kord.

3. Lõike 1 kohaselt saadud teabe põhjal koostab komisjon sertifitseeritud Euroopa digiidentiteedikukrute loetelu, avaldab selle *Euroopa Liidu Teatajas* ja hoiab seda masinloetavas formaadis.

4. Liikmesriik võib komisjonile esitada taotluse jätta Euroopa digiidentiteedikukkur ja e-identimise süsteem, mille alusel seda pakutakse, lõikes 3 osutatud loetelust välja.

5. Kui lõike 1 kohaselt esitatud teavet muudetakse, esitab liikmesriik komisjonile ajakohastatud teabe.

6. Komisjon ajakohastab lõikes 3 osutatud loetelu, avaldades vastavad muudatused *Euroopa Liidu Teatajas* ühe kuu jooksul alates lõike 4 kohase taotluse või lõike 5 kohase ajakohastatud teabe kättesaamisest.

7. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon käesoleva artikli lõigete 1, 4 ja 5 kohaldamisega seotud formaadid ja menetlused artikli 5a lõikes 23 osutatud rakendusaktidega, mis käsitlevad Euroopa digiidentiteedikukrute rakendamist. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 5e
Euroopa digiidentiteedikukrute turvarikkumine

1. Kui artikli 5a kohaselt pakutavate Euroopa digiidentiteedikukrute, artikli 5a lõikes 8 osutatud valideerimismehhanismi või e-identimise süsteemi, mille alusel pakutakse Euroopa digiidentiteedikukruid, turvalisust rikutakse või neid on osaliselt kahjustatud viisil, mis mõjutab nende usaldusväärsust või muude Euroopa digiidentiteedikukrute usaldusväärsust, peatab digiidentiteedikukruid kättesaadavaks teinud liikmesriik põhjendamatu viivituseta Euroopa digiidentiteedikukrute kättesaadavaks tegemise ja kasutamise.

   Liikmesriik kõrvaldab viivitamata Euroopa digiidentiteedikukrud kasutuselt, kui see on esimeses lõigus osutatud turvarikkumise või kahjustamise tõsidusest lähtudes põhjendatud.

Liikmesriik teavitab sellest mõjutatud kasutajaid, artikli 46c lõike 1 kohaselt määratud ühtseid kontaktpunkte, tuginevaid isikuid ja komisjoni.

2. Kui käesoleva artikli lõike 1 esimeses lõigus osutatud turvarikkumist või kahjustamist ei kõrvaldata kolme kuu jooksul alates peatamisest, kõrvaldab Euroopa digiidentiteedikukruid kättesaadavaks teinud liikmesriik Euroopa digiidentiteedikukrud kasutuselt ja tunnistab need kehtetuks. Liikmesriik teavitab mõjutatud kasutajaid sellisest kasutuselt kõrvaldamisest, artikli 46c lõike 1 kohaselt määratud ühtseid kontaktpunkte, tuginevaid isikuid ja komisjoni.

3. Pärast käesoleva artikli lõike 1 esimeses lõigus osutatud turvarikkumise või kahjustamise kõrvaldamist taastab digiidentiteedikukruid kättesaadavaks teinud liikmesriik Euroopa digiidentiteedikukrute kättesaadavaks tegemise ja kasutamise ning teavitab sellest põhjendamatu viivituseta mõjutatud kasutajaid ja tuginevaid isikuid, artikli 46c lõike 1 kohaselt määratud ühtset kontaktpunkti ja komisjoni.

4. Komisjon avaldab artiklis 5d osutatud loetelus tehtud vastavad muudatused põhjendamatu viivituseta *Euroopa Liidu Teatajas*.

5. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõigetes 1, 2 ja 3 osutatud meetmete jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 5f

Piiriülene tuginemine Euroopa digiidentiteedikukrutele

1. Kui liikmesriigid nõuavad avaliku sektori asutuse osutatavale internetipõhisele teenusele juurdepääsuks e-identimist ja e-autentimist, aktsepteerivad nad ka käesoleva määruse kohaselt pakutavaid Euroopa digiidentiteedikukruid.

2. Kui teenuseid osutavad erasektori tuginevad isikud, välja arvatud komisjoni soovituse 2003/361/EÜ*** lisa artiklis 2 määratletud mikroettevõtjad ja väikeettevõtjad, peavad liidu või riigisisese õiguse kohaselt kasutama veebis identimise korral tugevat kasutaja autentimist või kui tugev kasutaja autentimine veebis identimise korral on nõutav lepinguliste kohustuste kohaselt, muu hulgas sellistes valdkondades nagu transport, energeetika, pangandus, finantsteenused, sotsiaalkindlustus, tervishoid, joogivesi, postiteenused, digitaristu, haridus või telekommunikatsioon, peavad need erasektori tuginevad isikud hiljemalt 36 kuu möödumisel artikli 5a lõikes 23 ja artikli 5c lõikes 6 osutatud rakendusaktide jõustumisest ja üksnes kasutaja vabatahtliku taotluse korral aktsepteerima ka käesoleva määruse kohaselt pakutavaid Euroopa digiidentiteedikukruid.

3. Kui Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2065**** artiklis 33 osutatud väga suured digiplatvormid nõuavad kasutaja autentimist juurdepääsuks internetipõhistele teenustele, aktsepteerivad ja hõlbustavad nad kasutaja autentimiseks ka käesoleva määrusega kooskõlas pakutavate Euroopa digiidentiteedikukrute kasutamist üksnes kasutaja vabatahtliku taotluse korral ja selliste miinimumandmete osas, mida on vaja konkreetse internetipõhise teenuse jaoks, millega seoses autentimist nõutakse.

4. Komisjon hõlbustab koostöös liikmesriikidega tegevusjuhendite väljatöötamist tihedas koostöös kõigi asjaomaste sidusrühmadega, sealhulgas kodanikuühiskonnaga, et aidata kaasa Euroopa digiidentiteedikukrute laialdasele kättesaadavusele ja kasutatavusele käesoleva määruse kohaldamisalas ning julgustada teenuseosutajaid tegevusjuhendite väljatöötamise lõpule viima.

5. Komisjon hindab 24 kuu jooksul alates Euroopa digiidentiteedikukrute kasutuselevõtust Euroopa digiidentiteedikukrute nõudlust, kättesaadavust ja kasutatavust, võttes arvesse selliseid kriteeriume nagu kasutuselevõtt kasutajate poolt, teenuseosutajate piiriülene tegevus, tehnoloogia areng, kasutusharjumuste areng ja tarbijanõudlus.

---

* Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta direktiiv (EL) 2019/882 toodete ja teenuste ligipääsetavusnõuete kohta (ELT L 151, 7.6.2019, lk 70).

** Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

*** Komisjoni 6. mai 2003. aasta soovitus 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta (ELT L 124, 20.5.2003, lk 36).

**** Euroopa Parlamendi ja nõukogu 19. oktoobri 2022. aasta määrus (EL) 2022/2065, mis käsitleb digiteenuste ühtset turgu ja millega muudetakse direktiivi 2000/31/EÜ (digiteenuste määrus) (ELT L 277, 27.10.2022, lk 1).“

6) Artikli 6 ette lisatakse järgmine pealkiri:

„2. JAGU
E-IDENTIMISE SÜSTEEMID“.

7) Artikli 7 punkt g asendatakse järgmisega:

„g) vähemalt kuus kuud enne artikli 9 lõike 1 kohast teavitamist esitab teavitav liikmesriik teistele liikmesriikidele artikli 12 lõike 5 kohaldamise eesmärgil selle süsteemi kirjelduse artikli 12 lõikes 6 kohaselt vastu võetud rakendusaktidega kehtestatud menetluse kohaselt;“.

8) Artikli 8 lõike 3 esimene lõik asendatakse järgmisega:

„3. Võttes arvesse asjakohaseid rahvusvahelisi standardeid ja tingimusel, et järgitakse lõikes 2 sätestatut, kehtestab komisjon 18. septembriks 2015 rakendusaktidega minimaalsed tehnilised kirjeldused, standardid ja menetlused, mille suhtes määratakse e-identimise vahendite jaoks kindlaks madal, märkimisväärne või kõrge usaldusväärsuse tase.“

9) Artikli 9 lõiked 2 ja 3 asendatakse järgmisega:

„2. Komisjon avaldab põhjendamatu viivituseta *Euroopa Liidu Teatajas* nimekirja e-identimise süsteemidest, millest on teatatud vastavalt lõikele 1, ja nende süsteemidega seotud põhiteabe.

3. Komisjon avaldab lõikes 2 osutatud nimekirja muudatused *Euroopa Liidu Teatajas* ühe kuu jooksul pärast asjaomase teate saamist.“

10) Artikli 10 pealkiri asendatakse järgmisega:

„E-identimise süsteemide turvarikkumine“.

11) Lisatakse järgmine artikkel:

„*Artikkel 11a*
Piiriülene identiteedi ühitamine

1. Piiriüleste teenuste puhul tuginevate isikutena tegutsedes tagavad liikmesriigid füüsiliste isikute identiteedi ühese ühitamise, kasutades teavitatud e-identimise vahendit või Euroopa digiidentiteedikukruid.

2. Liikmesriigid näevad ette tehnilised ja korralduslikud meetmed, et tagada identiteedi ühitamiseks kasutatavate isikuandmete kõrgetasemeline kaitse ja vältida kasutajate profiilianalüüsi.

3. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõikes 1 osutatud nõuete jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

12) Artiklit 12 muudetakse järgmiselt:

a) artikli pealkiri asendatakse järgmisega:

„Koostalitlusvõime“;

b) lõiget 3 muudetakse järgmiselt:

i) punkt c asendatakse järgmisega:

„c) see hõlbustab lõimitud privaatsuse ja turbe rakendamist;“;

ii) punkt d jäetakse välja;

c) lõike 4 punkt d asendatakse järgmisega:

„d) viide e-identimise süsteemidest kättesaadavatele minimaalsele hulgale isikutuvastusandmetele, mis on vajalikud ainuüksi ühe füüsilise või juriidilise isiku või teist füüsilist isikut või juriidilist isikut esindava füüsilise isiku tähistamiseks;“;

d) lõiked 5 ja 6 asendatakse järgmisega:

„5. Liikmesriigid viivad läbi selliste e-identimise süsteemide vastastikuseid hindamisi, mis kuuluvad käesoleva määruse kohaldamisalasse ja millest tuleb teatada vastavalt artikli 9 lõike 1 punktile a.

6. Komisjon kehtestab 18. märtsiks 2025 rakendusaktidega käesoleva artikli lõikes 5 osutatud vastastikusteks hindamisteks vajaliku menetluse, et edendada usalduse ja turvalisuse kõrget taset, mis vastab riski suurusele. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“;

e) lõige 7 jäetakse välja;

f) lõige 8 asendatakse järgmisega:

„8. Selleks et näha ette ühtsed tingimused käesoleva artikli lõikest 1 tuleneva nõude rakendamiseks, võtab komisjon 18. septembriks 2025 käesoleva artikli lõikes 3 sätestatud kriteeriumide kohaselt ja liikmesriikidevahelise koostöö tulemusi arvesse võttes vastu rakendusaktid lõikes 4 sätestatud koostalitlusvõime raamistiku kohta. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

13) II peatükki lisatakse järgmised artiklid:

„*Artikkel 12a*

E-identimise süsteemide sertifitseerimine

1. Liikmesriikide määratud vastavushindamisasutused sertifitseerivad selliste e-identimise süsteemide, millest tuleb teatada, vastavust käesolevas määruses sätestatud küberturvalisuse nõuetele, sealhulgas vastavust artikli 8 lõikes 2 sätestatud küberturvalisuse seisukohast asjakohastele nõuetele seoses e-identimise süsteemide usaldusväärsuse tasemetega.

2. Käesoleva artikli lõike 1 kohane sertifitseerimine toimub määruse (EL) 2019/881 kohase asjaomase küberturvalisuse sertifitseerimise kava või selle osade alusel, niivõrd kui küberturvalisuse sertifikaat või selle osad hõlmavad kõnealuseid küberturvalisuse nõudeid.

3. Lõike 1 kohane sertifitseerimine kehtib kuni viis aastat, tingimusel et iga kahe aasta järel viiakse läbi nõrkuste hindamine. Kui tehakse kindlaks nõrkus ja seda ei kõrvaldata kolme kuu jooksul selle kindlakstegemisest, sertifitseerimine tühistatakse.

4. Olenemata lõikest 2 võivad liikmesriigid nõuda teavitavalt liikmesriigilt kooskõlas kõnealuse lõikega lisateavet sertifitseeritud e-identimise süsteemide või nende osade kohta.

5. Artikli 12 lõikes 5 osutatud e-identimise süsteemide vastastikust hindamist ei kohaldata käesoleva artikli lõike 1 kohaselt sertifitseeritud e-identimise süsteemide või nende osade suhtes. Liikmesriigid võivad artikli 8 lõikes 2 e-identimise süsteemide usaldusväärsuse taseme kohta sätestatud muude kui küberturvalisusega seotud nõuete puhul kasutada sertifikaati või vastavusdeklaratsiooni, mis on väljastatud asjakohase sertifitseerimise kava või selle osa alusel.

6. Liikmesriigid teatavad komisjonile lõikes 1 osutatud vastavushindamisasutuste nimed ja aadressid. Komisjon teeb selle teabe kõigile liikmesriikidele kättesaadavaks.

Artikkel 12b

Juurdepääs riist- ja tarkvarafunktsioonidele

Kui Euroopa digiidentiteedikukrute pakkujad ja teavitatud e-identimise vahendite väljastajad, kes tegutsevad äri- või kutsetegevuse raames ja kasutavad Euroopa Parlamendi ja nõukogu määruse (EL) 2022/1925* artikli 2 punktis 2 määratletud põhiplatvormiteenuseid Euroopa digiidentiteedikukru teenuste ja e-identimise vahendite pakkumiseks või selle käigus, on nimetatud määruse artikli 2 punktis 21 määratletud ärikasutajad, võimaldavad pääsuvalitsejad neile eelkõige tõhusa koostalitlusvõime samade operatsioonisüsteemi ja riist- või tarkvarafunktsioonidega ning koostalitlusvõime eesmärgil juurdepääsu sellistele funktsioonidele. Selline tõhus koostalitlusvõime ja juurdepääs on tasuta ega olene sellest, kas riist- või tarkvarafunktsioonid on osa operatsioonisüsteemist, mis on kättesaadavad kõnealusele pääsuvalitsejale ja mida ta kasutab selliste teenuste osutamisel, nagu on kirjeldatud määruse (EL) 2022/1925 artikli 6 lõikes 7. Käesolev artikkel ei piira käesoleva määruse artikli 5a lõike 14 kohaldamist.

---

* Euroopa Parlamendi ja nõukogu 14. septembri 2022. aasta määrus (EL) 2022/1925, mis käsitleb konkurentsile avatud ja õiglaseid turge digisektoris ning millega muudetakse direktiive (EL) 2019/1937 ja (EL) 2020/1828 (digiturgude määrus) (ELT L 265, 12.10.2022, lk 1).“

14) Artikli 13 lõige 1 asendatakse järgmisega:

„1. Olenemata käesoleva artikli lõikest 2 ja piiramata määruse (EL) 2016/679 kohaldamist, vastutavad usaldusteenuse osutajad füüsilisele või juriidilisele isikule tahtlikult või hooletusest tekitatud kahju eest, mis tuleneb käesolevas määruses sätestatud kohustuste täitmata jätmisest. Igal füüsilisel või juriidilisel isikul, kes on kandnud varalist või mittevaralist kahju seetõttu, et usaldusteenuse pakkuja on rikkunud käesolevat määrust, on õigus nõuda hüvitist kooskõlas liidu ja liikmesriigi õigusega.

Kvalifitseerimata usaldusteenuse osutaja tegevuse tahtlikkuse või hooletuse tõendamise kohustus lasub füüsilisel või juriidilisel isikul, kes väidab, et talle on põhjustatud esimeses lõigus osutatud kahju.

Eeldatakse, et kvalifitseeritud usaldusteenuse osutaja on tegutsenud tahtlikult või hooletult, kui nimetatud kvalifitseeritud usaldusteenuse osutaja ei tõenda, et esimeses lõigus osutatud kahju tekkis ilma selle kvalifitseeritud usaldusteenuse osutaja tahtliku või hooletu tegutsemiseta.“

15) Artiklid 14, 15 ja 16 asendatakse järgmisega:

„*Artikkel 14*
Rahvusvahelised aspektid

1. Kolmandas riigis või rahvusvahelise organisatsooni poolt asutatud usaldusteenuse osutajate pakutavaid usaldusteenuseid tunnistatakse õiguslikult samaväärsetena liidus asutatud kvalifitseeritud usaldusteenuse osutajate osutatavate kvalifitseeritud usaldusteenustega juhul, kui kolmandast riigist või rahvusvahelisest organisatsioonist pärit usaldusteenuseid tunnustatakse rakendusaktidega või ELi toimimise lepingu artikli 218 kohaselt liidu ja kolmanda riigi või rahvusvahelise organisatsiooni vahel sõlmitud lepingu alusel.

   Esimeses lõigus osutatud rakendusaktid võetakse vastu artikli 48 lõikes 2 osutatud kontrollimenetluse kohaselt.

2. Lõikes 1 osutatud rakendusaktide ja lepinguga tagatakse, et asjaomaste kolmandate riikide või rahvusvahelise organisatsiooni usaldusteenuse osutajad ning nende osutatavad usaldusteenused vastavad liidus asutatud kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate kvalifitseeritud usaldusteenuste suhtes kohaldatavatele nõuetele. Kolmandad riigid ja rahvusvahelised organisatsioonid koostavad eelkõige tunnustatud usaldusteenuse osutajate usaldusnimekirja ning haldavad seda ja avaldavad selle.

3. Lõikes 1 osutatud lepinguga tagatakse, et liidus asutatud kvalifitseeritud usaldusteenuse osutajate poolt osutatavaid kvalifitseeritud usaldusteenuseid tunnistatakse õiguslikult samaväärsetena usaldusteenustega, mida osutavad selle kolmanda riigi või rahvusvahelise organisatsiooni usaldusteenuse osutajad, kellega leping on sõlmitud.

Artikkel 15
Ligipääsetavus puuetega ja erivajadustega inimeste jaoks

E-identimise vahendite pakkumine ja usaldusteenuste osutamine ja nende teenuste osutamisel kasutatavad lõppkasutajatele suunatud tooted tehakse kättesaadavaks lihtsas ja arusaadavas keeles, kooskõlas ÜRO puuetega inimeste õiguste konventsiooniga ja direktiivis (EL) 2019/882 sätestatud ligipääsetavusnõuetega, tuues seega kasu ka piiratud funktsionaalse võimekusega inimestele, näiteks eakatele, ja isikutele, kellel on piiratud juurdepääs digitehnoloogiale.

Artikkel 16
Karistused

1. Liikmesriigid kehtestavad normid käesoleva määruse rikkumise eest kohaldatavate karistuste kohta, piiramata Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555* artikli 31 kohaldamist. Nimetatud karistused peavad olema mõjusad, proportsionaalsed ja hoiatavad.

2. Liikmesriigid tagavad, et kui kvalifitseeritud ja kvalifitseerimata usaldusteenuse osutaja rikub käesolevat määrust, määratakse selle eest haldustrahv, mille maksimummäär on vähemalt

   a) 5 000 000 eurot, kui usaldusteenuse osutaja on füüsiline isik, või

   b) kui usaldusteenuse osutaja on juriidiline isik, siis 5 000 000 eurot või 1 % selle ettevõtja üleilmsest aastasest kogukäibest, kuhu usaldusteenuse osutaja kuulus rikkumise toimumise aastale eelnenud majandusaastal, olenevalt sellest, kumb on suurem.

3. Olenevalt liikmesriikide õigussüsteemist võib haldustrahve käsitlevaid õigusnorme kohaldada selliselt, et trahvi määramise algatab pädev järelevalveasutus ja selle määrab riigi pädev kohus. Selliste normide kohaldamine nendes liikmesriikides tagab, et need õiguskaitsevahendid on tõhusad ja neil on järelevalveasutuste poolt otse määratud haldustrahvidega samaväärne mõju.

---

* Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80).“

16) III peatüki 2. jao pealkiri asendatakse järgmisega:

„Kvalifitseerimata usaldusteenused“.

17) Artiklid 17 ja 18 jäetakse välja.

18) III peatüki 2. jakku lisatakse järgmine artikkel:

„*Artikkel 19a*
Nõuded kvalifitseerimata usaldusteenuse osutajatele

1. Kvalifitseerimata usaldusteenuseid osutav kvalifitseerimata usaldusteenuse osutaja

a) evib asjakohaseid tegevuspõhimõtteid ja võtab vastavaid meetmeid, et juhtida kvalifitseerimata usaldusteenuse osutamisega seotud õiguslikke, ärilisi, tegevus- ja muid otseseid või kaudseid riske, mis olenemata direktiivi (EL) 2022/2555 artiklist 18 hõlmavad vähemalt meetmeid, mis on seotud

i) usaldusteenuse kasutamise registreerimise ja teenuse aktiveerimise menetlustega;

ii) usaldusteenuste osutamiseks vajalike menetlus- või halduskontrollidega;

iii) usaldusteenuste haldamise ja rakendamisega;

b) teavitab järelevalveasutust, tuvastatavaid mõjutatud isikuid, üldsust, kui see on avalikes huvides, ja kui see on kohaldatav, teisi asjaomaseid pädevaid asutusi kõigist sellistest teenuse osutamisel või punkti a alapunktis i, ii või iii osutatud meetmete rakendamisel esinenud turvarikkumistest või häiretest, millel on märkimisväärne mõju osutatavale usaldusteenusele või sellega seoses säilitatavatele isikuandmetele, tehes seda põhjendamatu viivituseta ja igal juhul 24 tunni jooksul turvarikkumisest või häirest teada saamist.

2. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõike 1 punkti a kohaldamiseks. Kui neid standardeid, kirjeldusi ja menetlusi järgitakse, loetakse käesolevas artiklis sätestatud nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

19) Artiklit 20 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Vastavushindamisasutus auditeerib kvalifitseeritud usaldusteenuse osutajaid nende oma kulul vähemalt iga 24 kuu järel. Auditiga kinnitatakse, et kvalifitseeritud usaldusteenuse osutajad ja nende osutatavad kvalifitseeritud usaldusteenused vastavad käesolevas määruses ja direktiivi (EL) 2022/2555 artiklis 21 sätestatud nõuetele. Kvalifitseeritud usaldusteenuse osutajad esitavad saadud vastavushindamisaruande järelevalveasutusele kolme tööpäeva jooksul alates selle kättesaamisest.“;

b) lisatakse järgmised lõiked:

„1a. Kvalifitseeritud usaldusteenuse osutajad teavitavad järelevalveasutust kavandatud audititest vähemalt üks kuu ette ja võimaldavad järelevalveasutusel taotluse korral neis vaatlejana osaleda.

1b. Liikmesriigid teatavad põhjendamatu viivituseta komisjonile lõikes 1 osutatud vastavushindamisasutuste nimed, aadressid ja akrediteerimisandmed ning nende hilisemad muudatused. Komisjon teeb selle teabe kõigile liikmesriikidele kättesaadavaks.“;

c) lõiked 2, 3 ja 4 asendatakse järgmisega:

„2. Ilma et see piiraks lõike 1 kohaldamist, võib järelevalveasutus kvalifitseeritud usaldusteenuse osutajate kulul auditeerida või nõuda vastavushindamisasutusel teha kõnealuste kvalifitseeritud usaldusteenuse osutajate vastavushindamise, et kinnitada kvalifitseeritud usaldusteenuse osutajate ning tema poolt osutatavate kvalifitseeritud usaldusteenuste vastavust käesolevas määruses sätestatud nõuetele. Kui isikuandmete kaitse reegleid näib olevat rikutud, teavitab järelevalveasutus põhjendamatu viivituseta määruse (EL) 2016/679 artikli 51 kohaselt asutatud pädevaid järelevalveasutusi.

3. Kui kvalifitseeritud usaldusteenuse osutaja ei täida mõnda käesolevas määruses sätestatud nõuet, nõuab järelevalveasutus, et ta võtaks kindlaksmääratud tähtaja jooksul, kui see on kohaldatav, heastamismeetmeid.

Kui asjaomane teenuseosutaja ei võta heastamismeetmeid järelevalveasutuse kehtestatud tähtaja jooksul, kui see on kohaldatav, võtab järelevalveasutus, kui seda õigustavad eelkõige kõnealuse nõuete täitmata jätmise ulatus, kestus ja tagajärjed, sellelt teenuseosutajalt või tema osutatavalt mõjutatud teenuselt kvalifitseeritud staatuse ära.

3a. Kui direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud või asutatud pädevad asutused teatavad järelevalveasutusele, et kvalifitseeritud usaldusteenuse osutaja ei täida mõnda nimetatud direktiivi artiklis 21 sätestatud nõuet, võtab järelevalveasutus, kui seda õigustavad eelkõige kõnealuse nõuete täitmata jätmise ulatus, kestus ja tagajärjed, kõnealuselt teenuseosutajalt või tema osutatavalt mõjutatud teenuselt kvalifitseeritud staatuse ära.

3b. Kui määruse (EL) 2016/679 artikli 51 kohaselt asutatud järelevalveasutused teatavad järelevalveasutusele, et kvalifitseeritud usaldusteenuse osutaja ei täida mõnda nimetatud määruses sätestatud nõuet, võtab järelevalveasutus, kui seda õigustavad eelkõige kõnealuse nõuete täitmata jätmise ulatus, kestus ja tagajärjed, kõnealuselt teenuseosutajalt või tema osutatavalt mõjutatud teenuselt kvalifitseeritud staatuse ära.

3c. Järelevalveasutus teavitab kvalifitseeritud usaldusteenuse osutajat temalt või asjaomaselt teenuselt kvalifitseeritud staatuse äravõtmisest. Järelevalveasutus teavitab käesoleva määruse artikli 22 lõike 3 kohaselt teatatud asutust, et ajakohastada kõnealuse artikli lõikes 1 osutatud usaldusnimekirju, ning direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud või asutatud pädevat asutust.

4. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused järgmise jaoks:

a) vastavushindamisasutuste akrediteerimine ja lõikes 1 osutatud vastavushindamisaruanne;

b) auditeerimisnõuded, mille alusel vastavushindamisasutused hindavad, sealhulgas kompleksse hindamise vormis, kvalifitseeritud usaldusteenuse osutajate nõuetele vastavust, nagu on osutatud lõikes 1;

c) vastavushindamissüsteemid kvalifitseeritud usaldusteenuse osutajate vastavushindamiseks vastavushindamisasutuste poolt ja lõikes 1 osutatud aruande esitamiseks.

Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

20) Artiklit 21 muudetakse järgmiselt:

a) lõiked 1 ja 2 asendatakse järgmisega:

„1. Kui usaldusteenuse osutajad kavatsevad alustada kvalifitseeritud usaldusteenuse osutamist, teavitavad nad järelevalveasutust oma kavatsusest ning esitavad selle teabega koos vastavushindamisasutuse koostatud vastavushindamisaruande, milles kinnitatakse käesolevas määruses ja direktiivi (EL) 2022/2555 artiklis 21 sätestatud nõuete täitmist.

2. Järelevalveasutus kontrollib usaldusteenuse osutaja ja tema osutatavate usaldusteenuste vastavust käesolevas määruses sätestatud nõuetele ning eelkõige kvalifitseeritud usaldusteenuse osutajatele ja nende osutatavatele kvalifitseeritud usaldusteenustele kehtestatud nõuetele.

Et kontrollida usaldusteenuse osutaja vastavust direktiivi (EL) 2022/2555 artikli 21 nõuetele, taotleb järelevalveasutus, et kõnealuse direktiivi artikli 8 lõike 1 kohaselt määratud või asutatud pädevad asutused võtaksid sellega seoses järelevalvemeetmeid ja esitaksid tulemuste kohta teabe põhjendamatu viivituseta ja igal juhul kahe kuu jooksul pärast taotluse saamist. Kui kahe kuu jooksul alates teavitamisest ei ole kontrolli lõpule viidud, teavitavad asjaomased pädevad asutused järelevalveasutust viivituse põhjustest ja ajavahemikust, mille jooksul kontroll lõpule viiakse.

Kui järelevalveasutus leiab, et usaldusteenuse osutaja ja tema osutatavad usaldusteenused vastavad käesolevas määruses sätestatud nõuetele, annab järelevalveasutus usaldusteenuse osutajale ja tema osutatavatele usaldusteenustele kvalifitseeritud staatuse ning teavitab artikli 22 lõikes 3 osutatud asutust artikli 22 lõikes 1 osutatud usaldusnimekirjade ajakohastamise eesmärgil hiljemalt kolme kuu möödumisel käesoleva artikli lõike 1 kohast teate esitamisest.

Kui kolme kuu jooksul alates teate esitamisest ei ole kontrolli lõpule viidud, teavitab järelevalveasutus usaldusteenuse osutajat viivituse põhjustest ja ajavahemikust, mille jooksul kontroll lõpule viiakse.“;

b) lõige 4 asendatakse järgmisega:

„4. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega teavitamise ja kontrolli formaadid ja menetlused käesoleva artikli lõigete 1 ja 2 kohaldamiseks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

21) Artiklit 24 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Kvalifitseeritud sertifikaati või kvalifitseeritud elektroonilist tõendit väljastades kontrollib kvalifitseeritud usaldusteenuse osutaja selle füüsilise või juriidilise isiku identiteeti, ja kui see on kohaldatav, konkreetseid atribuute, kellele kvalifitseeritud sertifikaat või kvalifitseeritud elektrooniline tõend väljastatakse.

1a. Kvalifitseeritud usaldusteenuse osutaja teeb lõikes 1 osutatud identiteedikontrolli asjakohasel viisil kas otse või kolmanda isiku abil, lähtudes ühest järgmisest meetodist või vajaduse korral nende kombinatsioonist kooskõlas lõikes 1c osutatud rakendusaktidega:

a) Euroopa digiidentiteedikukru või teavitatud e-identimise vahendi abil, mis vastab artiklis 8 sätestatud nõuetele seoses kõrge usaldusväärsuse tasemega;

b) kooskõlas punktiga a, c või d väljastatud kvalifitseeritud e-allkirja sertifikaadi või kvalifitseeritud e-templi sertifikaadi abil;

c) muude identimismeetodite abil, mis tagavad isiku tuvastamise kõrgel usaldusväärsuse tasemel ja mille vastavust kinnitab vastavushindamisasutus;

d) füüsilise isiku või juriidilise isiku volitatud esindaja füüsilise kohalolekuga vastavalt asjakohastele tõenditele ja, menetlustele kooskõlas riigisisese õigusega.

1b. Kvalifitseeritud usaldusteenuse osutaja teeb lõikes 1 osutatud atribuutide kontrolli asjakohasel viisil kas otse või kolmanda isiku abil, lähtudes ühest järgmisest meetodist või vajaduse korral nende kombinatsioonist kooskõlas lõikes 1c osutatud rakendusaktidega

a) Euroopa digiidentiteedikukru või teavitatud e-identimise vahendi abil, mis vastab artiklis 8 sätestatud nõuetele seoses kõrge usaldusväärsuse tasemega;

b) kooskõlas lõike 1a punktiga a, c või d väljastatud kvalifitseeritud e-allkirja sertifikaadi või kvalifitseeritud e-templi sertifikaadi abil;

c) kvalifitseeritud elektroonilise tõendi abil;

d) muude meetodite abil, mis tagavad atribuutide kontrollimise tulemuste kõrge usaldusväärsuse taseme ja mille vastavust kinnitab vastavushindamisasutus;

e) füüsilise isiku või juriidilise isiku volitatud esindaja füüsilise kohalolekuga vastavalt asjakohastele tõenditele ja menetlustele kooskõlas riigisisese õigusega.

1c. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused identiteedi ja atribuutide kontrollimiseks kooskõlas käesoleva artikli lõigetega 1, 1a ja 1b. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega. “;

b) lõiget 2 muudetakse järgmiselt:

i) punkt a asendatakse järgmisega:

„a) teavitab järelevalveasutust vähemalt üks kuu ette enne mis tahes muudatuse rakendamist oma kvalifitseeritud usaldusteenuste osutamisel või vähemalt kolm kuud ette enne, kui on kavatsus selline tegevus lõpetada.“;

ii) punktid d ja e asendatakse järgmisega:

„d) teavitab enne lepingu sõlmimist kõiki kvalifitseeritud usaldusteenust kasutada soovivaid isikuid selgel, põhjalikul ja hõlpsasti ligipääsetaval viisil, avalikult ligipääsetavas ruumis ja isiklikult kõnealuse teenuse kasutamise täpsetest tingimustest, sealhulgas kõigist selle kasutamise piirangutest;

e) kasutab usaldusväärseid süsteeme ja tooteid, mis on kaitstud muutmise eest, ja tagab nende toetatavate toimingute tehnilise turvalisuse ja usaldusväärsuse, sealhulgas kasutades sobivaid krüptomeetodeid;“;

iii) lisatakse järgmised punktid:

„fa) olenemata direktiivi (EL) 2022/2555 artiklis 21 sätestatust, evib asjakohaseid tegevuspõhimõtteid ja võtab vastavaid meetmeid, et juhtida kvalifitseeritud usaldusteenuse osutamisega seotud õiguslikke, ärilisi, tegevus- ja muid otseseid või kaudseid riske, sealhulgas vähemalt meetmeid, mis on seotud järgmisega:

i) teenuse kasutamiseks registreerimise ja teenuse aktiveerimise menetlused;

ii) menetlus- või halduskontrollid;

iii) teenuste haldamine ja rakendamine;

fb) teavitab järelevalveasutust, tuvastatavaid mõjutatud isikuid, kohaldataval juhul teisi asjaomaseid pädevaid asutusi ning järelevalveasutuse taotlusel ka üldsust, kui see on avalikes huvides, kõigist sellistest teenuse osutamisel või punkti fa alapunktis i, ii või iii osutatud meetmete rakendamisel esinenud turvarikkumistest või häiretest, millel on märkimisväärne mõju osutatavale usaldusteenusele või sellega seoses säilitatavatele isikuandmetele, tehes seda põhjendamatu viivituseta ja igal juhul 24 tunni jooksul pärast intsidenti;“

iv) punktid g, h ja i asendatakse järgmisega:

„g) võtab asjakohaseid meetmeid andmete võltsimise, varguse või omastamise vastu või andmete loata kustutamise, muutmise või ligipääsmatuks muutmise vastu;

h) salvestab kogu asjakohase teabe kvalifitseeritud usaldusteenuse osutaja väljastatud ja saadud andmete kohta ja hoiab seda kättesaadavana vajaliku aja jooksul pärast seda, kui kvalifitseeritud usaldusteenuse osutaja on tegevuse lõpetanud, et esitada tõendeid kohtumenetlustes ja tagada teenuse järjepidevus. Sellised andmed võib salvestada elektrooniliselt;

i) omab teenuse järjepidevuse tagamiseks ajakohast tegevuse lõpetamise kava, mis vastab järelevalveasutuse poolt artikli 46b lõike 4 punkti i kohaselt kontrollitud sätetele;“;

v) punkt j jäetakse välja;

vi) lisatakse järgmine lõik:

„Järelevalveasutus võib nõuda täiendavat teavet lisaks esimese lõigu punkti a kohaselt esitatud teabele või vastavushindamise tulemusi ning võib kehtestada tingimusi kvalifitseeritud usaldusteenustes kavandatud muudatuste tegemiseks loa andmiseks. Kui kolme kuu jooksul alates teate esitamisest ei ole kontrolli lõpule viidud, teavitab järelevalveasutus usaldusteenuse osutajat viivituse põhjustest ja ajavahemikust, mille jooksul kontroll lõpule viiakse.“;

c) lõige 5 asendatakse järgmisega:

„4a. Kvalifitseeritud elektrooniliste tõendite kehtetuks tunnistamise suhtes kohaldatakse vastavalt lõikeid 3 ja 4.

4b. Komisjonil on õigus võtta kooskõlas artikliga 47 vastu delegeeritud õigusakte, millega kehtestatakse käesoleva artikli lõike 2 punktis fa osutatud täiendavad meetmed.

5. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõikes 2 osutatud nõuete jaoks. Kui neid standardeid, kirjeldusi ja menetlusi järgitakse, loetakse käesolevas lõikes sätestatud nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

22) III peatüki 3. jakku lisatakse järgmine artikkel:

„*Artikkel 24a*

Kvalifitseeritud usaldusteenuste tunnustamine

1. Ühes liikmesriigis väljastatud kvalifitseeritud sertifikaadil põhinevaid kvalifitseeritud e-allkirju ja ühes liikmesriigis väljastatud kvalifitseeritud sertifikaadil põhinevaid kvalifitseeritud e-templeid tunnustatakse vastavalt kvalifitseeritud e-allkirjadena ja kvalifitseeritud e-templitena ka kõigis teistes liikmesriikides.

2. Ühes liikmesriigis sertifitseeritud kvalifitseeritud e-allkirja andmise vahendeid ja kvalifitseeritud e-templi loomise vahendeid tunnustatakse vastavalt kvalifitseeritud e-allkirja andmise vahenditena ja kvalifitseeritud e-templi loomise vahenditena ka kõigis teistes liikmesriikides.

3. Ühes liikmesriigis pakutavat e-allkirjade kvalifitseeritud sertifikaati, e-templite kvalifitseeritud sertifikaati, kvalifitseeritud usaldusteenust kvalifitseeritud e-allkirja kaugloomise vahendite haldamiseks ja kvalifitseeritud usaldusteenust kvalifitseeritud e-templi vahemaa tagant loomise vahendite haldamiseks tunnustatakse vastavalt e-allkirjade kvalifitseeritud sertifikaadina, e-templite kvalifitseeritud sertifikaadina, kvalifitseeritud usaldusteenusena kvalifitseeritud e-allkirja kaugloomise vahendite haldamiseks ja kvalifitseeritud usaldusteenusena kvalifitseeritud e-templite vahemaa tagant loomise vahendite haldamiseks ka kõigis teistes liikmesriikides.

4. Ühes liikmesriigis pakutavat kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenust ja kvalifitseeritud e-templite kvalifitseeritud valideerimisteenust tunnustatakse kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenusena ja kvalifitseeritud e-templite kvalifitseeritud valideerimisteenusena ka kõigis teistes liikmesriikides.

5. Ühes liikmesriigis pakutavat kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenust ja kvalifitseeritud e-templite kvalifitseeritud säilitamisteenust tunnustatakse kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenusena ja kvalifitseeritud e-templite kvalifitseeritud säilitamisteenusena ka kõigis teistes liikmesriikides.

6. Ühes liikmesriigis pandud kvalifitseeritud e-ajatemplit tunnustatakse kvalifitseeritud e-ajatemplina ka kõigis teistes liikmesriikides.

7. Ühes liikmesriigis väljastatud kvalifitseeritud sertifikaati veebisaidi autentimiseks tunnustatakse kvalifitseeritud sertifikaadina veebisaidi autentimiseks ka kõigis teistes liikmesriikides.

8. Ühes liikmesriigis pakutavat kvalifitseeritud registreeritud e-andmevahetusteenust tunnustatakse kvalifitseeritud registreeritud e-andmevahetusteenusena ka kõigis teistes liikmesriikides.

9. Ühes liikmesriigis väljastatud kvalifitseeritud elektroonilist tõendit tunnustatakse kvalifitseeritud elektroonilise tõendina ka kõigis teistes liikmesriikides.

10. Ühes liikmesriigis pakutavat kvalifitseeritud elektroonilise arhiveerimise teenust tunnustatakse kvalifitseeritud elektroonilise arhiveerimise teenusena ka kõigis teistes liikmesriikides.

11. Ühes liikmesriigis kättesaadavat kvalifitseeritud elektroonilist arvestusraamatut tunnustatakse kvalifitseeritud elektroonilise arvestusraamatuna ka kõigis teistes liikmesriikides.“

23) Artikli 25 lõige 3 jäetakse välja.

24) Artiklit 26 muudetakse järgmiselt:

a) ainus lõik muudetakse lõikeks 1;

b) lisatakse järgmine lõige:

„2. Hiljemalt ... [24 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] hindab komisjon, kas on vaja võtta vastu rakendusakte, millega kehtestatakse võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused täiustatud e-allkirjade jaoks. Olenevalt hindamise tulemustest võib komisjon sellised rakendusaktid vastu võtta. Kui täiustatud e-allkiri vastab standarditele, kirjeldustele ja menetlustele, loetakse täiustatud e-allkirjadele esitatavad nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

25) Artikli 27 lõige 4 jäetakse välja.

26) Artikli 28 lõige 6 asendatakse järgmisega:

„6. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused e-allkirja kvalifitseeritud sertifikaatide jaoks. Kui e-allkirja kvalifitseeritud sertifikaat vastab kõnealustele standarditele, kirjeldustele ja menetlustele, loetakse I lisas sätestatud nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

27) Artiklisse 29 lisatakse järgmine lõige:

„1a. E-allkirja andmiseks vajalikke andmeid luuakse, hallatakse või varundamise eesmärgil dubleeritakse üksnes allkirja andja nimel, allkirja andja taotlusel ja kvalifitseeritud usaldusteenuse osutaja poolt, kes osutab kvalifitseeritud usaldusteenust kvalifitseeritud e-allkirja kaugloomise vahendi haldamiseks.“

28) Lisatakse järgmine artikkel:

„*Artikkel 29a*

Nõuded kvalifitseeritud e-allkirja kaugloomise vahendi haldamise kvalifitseeritud teenusele

1. Kvalifitseeritud e-allkirja kaugloomise vahendit haldab kvalifitseeritud teenuse osutamise raames üksnes kvalifitseeritud usaldusteenuse osutaja, kes

   a) allkirja andja nimel loob või haldab e-allkirja andmiseks vajalikke andmeid;

   b) olenemata II lisa punkti 1 alapunktist d dubleerib e-allkirja andmiseks vajalikke andmeid üksnes varundamise eesmärgil, kui on täidetud järgmised nõuded:

      i) dubleeritud andmekogumite turvatase peab olema sama mis algsetel andmekogumitel;

      ii) dubleeritud andmekogumite arv ei tohi ületada teenuse järjepidevuse tagamiseks vajalikku miinimumi;

   c) vastab kõigile nõuetele, mis on kindlaks määratud artikli 30 kohaselt väljastatud konkreetse kvalifitseeritud e-allkirja kaugloomise vahendi sertifitseerimise aruandes.

2. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõike 1 kohaldamiseks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

29) Artiklisse 30 lisatakse järgmine lõige:

„3a. Lõikes 1 osutatud sertifitseerimine kehtib maksimaalselt viis aastat, tingimusel et nõrkusi hinnatakse iga kahe aasta tagant. Kui tehakse kindlaks nõrkused ja neid ei kõrvaldata, siis sertifitseerimine tühistatakse.“

30) Artikli 31 lõige 3 asendatakse järgmisega:

„3. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega formaadid ja menetlused käesoleva artikli lõike 1 kohaldamiseks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

31) Artiklit 32 muudetakse järgmiselt:

a) lõikesse 1 lisatakse järgmine lõik:

„Kui kvalifitseeritud e-allkirjade valideerimine vastab lõikes 3 osutatud standarditele, kirjeldustele ja menetlustele, loetakse käesoleva lõike esimeses lõigus osutatud nõuded täidetuks.“;

b) lõige 3 asendatakse järgmisega:

„3. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused kvalifitseeritud e-allkirjade valideerimiseks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

32) Lisatakse järgmine artikkel:

„*Artikkel 32a*
Nõuded kvalifitseeritud sertifikaatidel põhinevate täiustatud e-allkirjade valideerimisele

1. Kvalifitseeritud sertifikaadil põhineva täiustatud e-allkirja valideerimise protsess kinnitab kvalifitseeritud sertifikaadil põhineva täiustatud e-allkirja kehtivust, kui on täidetud järgmised tingimused:

a) allkirja toetav sertifikaat oli allkirja andmise ajal I lisa nõuetele vastav e-allkirja kvalifitseeritud sertifikaat;

b) kvalifitseeritud sertifikaadi väljastas kvalifitseeritud usaldusteenuse osutaja ja sertifikaat oli allkirja andmise ajal kehtiv;

c) allkirja valideerimise andmed vastavad tuginevale isikule esitatud andmetele;

d) sertifikaadil allkirja andjat tähistavad kordumatud andmed on nõuetekohaselt esitatud tuginevale isikule;

e) kui allkirja andmisel kasutati varjunime, on varjunime kasutus tuginevale isikule selgesti näidatud;

f) allkirjastatud andmete terviklust ei ole kahjustatud;

g) artiklis 26 sätestatud nõuded olid allkirja andmise ajal täidetud.

2. Kvalifitseeritud sertifikaadil põhineva täiustatud e-allkirja valideerimiseks kasutatav süsteem annab tuginevale isikule valideerimisprotsessi korrektse tulemuse ja võimaldab tugineval isikul tuvastada turvalisusega seotud probleeme.

3. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused kvalifitseeritud sertifikaatidel põhinevate täiustatud e-allkirjade valideerimiseks. Kui kvalifitseeritud sertifikaatidel põhinevate täiustatud e-allkirjade valideerimine vastab kõnealustele standarditele, kirjeldustele ja menetlustele, loetakse see käesoleva artikli lõikes 1 sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

33) Artikli 33 lõige 2 asendatakse järgmisega:

„2. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõikes 1 osutatud kvalifitseeritud valideerimisteenuse jaoks. Kui kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenus vastab kõnealustele standarditele, kirjeldustele ja menetlustele, loetakse see käesoleva artikli lõikes 1 sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

34) Artiklit 34 muudetakse järgmiselt:

a) lisatakse järgmine lõige:

„1a. Kui kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenuse suhtes kohaldatav kord vastab lõikes 2 osutatud standarditele, kirjeldustele ja menetlustele, loetakse lõikes 1 sätestatud nõuded täidetuks.“;

b) lõige 2 asendatakse järgmisega:

„2. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenuse jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega. “

35) Artikli 35 lõige 3 jäetakse välja.

36) Artiklit 36 muudetakse järgmiselt:

a) ainus lõik muudetakse lõikeks 1;

b) lisatakse järgmine lõige:

„2. Hiljemalt ... [24 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] hindab komisjon, kas on vaja võtta vastu rakendusaktid, et kehtestada võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused täiustatud e-templite jaoks. Olenevalt hindamise tulemustest võib komisjon sellised rakendusaktid vastu võtta. Kui täiustatud e-tempel vastab kõnealustele standarditele, kirjeldustele ja menetlustele, loetakse täiustatud e-templitele esitatavad nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

37) Artikli 37 lõige 4 jäetakse välja.

38) Artikli 38 lõige 6 asendatakse järgmisega:

„6. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused e-templite kvalifitseeritud sertifikaatide jaoks. Kui e-templi kvalifitseeritud sertifikaat vastab kõnealustele standarditele, kirjeldustele ja menetlustele, loetakse III lisas sätestatud nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

39) Lisatakse järgmine artikkel:

„*Artikkel 39a*
Nõuded kvalifitseeritud e-templi kaugloomise vahendi haldamise kvalifitseeritud teenusele

Kvalifitseeritud e-templi kaugloomise vahendi haldamise kvalifitseeritud teenuse suhtes kohaldatakse *mutatis mutandis* artiklit 29a.“

40) III peatüki 5. jakku lisatakse järgmine artikkel:

„*Artikkel 40a*
Nõuded kvalifitseeritud sertifikaatidel põhinevate täiustatud e-templite valideerimisele

Kvalifitseeritud sertifikaatidel põhinevate täiustatud e-templite valideerimise suhtes kohaldatakse *mutatis mutandis* artiklit 32a.“

41) Artikli 41 lõige 3 jäetakse välja.

42) Artiklit 42 muudetakse järgmiselt:

a) lisatakse järgmine lõige:

„1a. Kui kuupäeva ja ajahetke andmetega sidumine ning ajaallika täpsus vastavad lõikes 2 osutatud standarditele, kirjeldustele ja menetlustele, loetakse lõikes 1 sätestatud nõuded täidetuks.“;

b) lõige 2 asendatakse järgmisega:

„2. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused kuupäeva ja ajahetke andmetega sidumiseks ning ajaallikate täpsuse kindlakstegemiseks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega. “

43) Artiklit 44 muudetakse järgmiselt:

a) lisatakse järgmine lõige:

„1a. Kui andmete saatmise ja kättesaamise protsess vastab lõikes 2 osutatud standarditele, kirjeldustele ja menetlustele, loetakse lõikes 1 sätestatud nõuded täidetuks.“;

b) lõige 2 asendatakse järgmisega:

„2. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused andmete saatmise ja kättesaamise protsesside jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega. “;

c) lisatakse järgmised lõiked:

„2a. Kvalifitseeritud registreeritud e-andmevahetusteenuste osutajad võivad kokku leppida nende osutatavate kvalifitseeritud registreeritud e-andmevahetusteenuste koostalitlusvõimes. Selline koostalitlusvõime raamistik peab vastama lõikes 1 sätestatud nõuetele ja selle vastavuse kinnitab vastavushindamisasutus.

2b. Komisjon võib rakendusaktidega kehtestada võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõikes 2a osutatud koostalitlusvõime raamistiku jaoks. Tehnilised kirjeldused ja standardite sisu peavad olema kulutõhusad ja proportsionaalsed. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

44) Artikkel 45 asendatakse järgmisega:

„*Artikkel 45*

Nõuded veebisaidi autentimise kvalifitseeritud sertifikaatidele

1. Veebisaidi autentimise kvalifitseeritud sertifikaadid peavad vastama IV lisas sätestatud nõuetele. Kõnealustele nõuetele vastavust hinnatakse vastavalt käesoleva artikli lõikes 2 osutatud standarditele, kirjeldustele ja menetlustele.

1a. Veebibrauserite pakkujad tunnustavad käesoleva artikli lõike 1 kohaselt väljastatud veebisaidi autentimise kvalifitseeritud sertifikaate. Veebibrauserite pakkujad tagavad, et sertifikaadis tõendatud identiteediandmed ja täiendavad tõendatud atribuudid kuvatakse kasutajasõbralikul viisil. Veebibrauserite pakkujad tagavad käesoleva artikli lõikes 1 osutatud veebisaidi autentimise kvalifitseeritud sertifikaatide toetamise ja koostalitlusvõime nendega; välja arvatud soovituse 2003/361/EÜ lisa artiklis 2 määratletud mikro- ja väikeettevõtjate puhul esimese viie aasta jooksul, mil nad tegutsevad veebilehitsemisteenuste pakkujatena.

1b. Veebisaidi autentimise kvalifitseeritud sertifikaatide suhtes ei kohaldata ühtegi kohustuslikku nõuet peale lõikes 1 sätestatud nõuete.

2. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõikes 1 osutatud veebisaidi autentimise kvalifitseeritud sertifikaatide jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

45) Lisatakse järgmine artikkel:

„*Artikkel 45a*
Ettevaatusabinõud küberturvalisuse tagamiseks

1. Veebibrauserite pakkujad ei võta abinõusid, mis on vastuolus nende artiklis 45 sätestatud kohustustega, eelkõige nõuetega tunnustada veebisaidi autentimiseks kvalifitseeritud sertifikaate ja kuvada esitatud identiteediandmeid kasutajasõbralikul viisil.

2. Erandina lõikest 1 ja üksnes põhjendatud kahtluse korral seoses tuvastatud sertifikaadi või sertifikaatide kogumi turvarikkumiste või tervikluse kadumisega võivad veebibrauserite pakkujad võtta asjaomase sertifikaadi või sertifikaatide kogumi suhtes ettevaatusabinõusid.

3. Kui veebibrauserite pakkuja võtab lõike 2 kohaselt ettevaatusabinõusid, teatab veebibrauserite pakkuja oma kahtlustest põhjendamatu viivituseta kirjalikult komisjonile, pädevale järelevalveasutusele, üksusele, kellele sertifikaat väljastati, ja kvalifitseeritud usaldusteenuse osutajale, kes asjaomase sertifikaadi või sertifikaatide kogumi väljastas. Sellise teate saamisel saadab pädev järelevalveasutus asjaomasele veebibrauserite pakkujale kinnituse teate kättesaamise kohta.

4. Pädev järelevalveasutus uurib teates tõstatatud küsimusi kooskõlas artikli 46b lõike 4 punktiga k. Kui uurimise tulemusel sertifikaadi kvalifitseeritud staatust ära ei võeta, teavitab järelevalveasutus sellest veebibrauserite pakkujat ja palub tal lõpetada käesoleva artikli lõikes 2 osutatud ettevaatusabinõude rakendamise.“

46) III peatükki lisatakse järgmised jaod:

„9. JAGU
ELEKTROONILINE TÕEND

Artikkel 45b
Elektroonilise tõendi õiguslik toime

1. Elektroonilise tõendi õigusjõudu ega kohtumenetluses tõendina lubatavust ei tohi välistada üksnes seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud elektroonilistele tõenditele esitatavatele nõuetele.

2. Kvalifitseeritud elektroonilistel tõenditel ja tõenditel, mis on välja antud autentse allika eest vastutava avaliku sektori asutuse poolt või nimel, on samasugune õiguslik toime nagu seaduslikult välja antud paberil tõenditel.

3. Tõendit, mis on ühes liikmesriigis väljastatud autentse allika eest vastutava avaliku sektori asutuse poolt või nimel, tunnustatakse tõendina, mis on väljastatud autentse allika eest vastutava avaliku sektori asutuse poolt või nimel, kõigis liikmesriikides.

Artikkel 45c

Elektrooniline tõend avalike teenuste puhul

Kui vastavalt riigisisesele õigusele nõutakse avaliku sektori asutuse osutatavale internetipõhisele teenusele juurdepääsuks elektroonilist tuvastamist e-identimise vahendi abil ja autentimist, ei asenda elektroonilises tõendis sisalduvad isikutuvastusandmed elektroonilist tuvastamist e-identimise vahendi abil ja autentimist elektroonilise tuvastamise eesmärgil, välja arvatud juhul, kui liikmesriik seda konkreetselt lubab. Sellisel juhul aktsepteeritakse ka teiste liikmesriikide kvalifitseeritud elektroonilisi tõendeid.

Artikkel 45d

Kvalifitseeritud elektroonilistele tõenditele esitatavad nõuded

1. Kvalifitseeritud elektrooniline tõend peab vastama V lisas sätestatud nõuetele.

2. V lisas sätestatud nõuetele vastavust hinnatakse vastavalt käesoleva artikli lõikes 5 osutatud standarditele, kirjeldustele ja menetlustele.

3. Kvalifitseeritud elektroonilise tõendi suhtes ei kohaldata ühtegi kohustuslikku nõuet lisaks V lisas sätestatud nõuetele.

4. Kui kvalifitseeritud elektrooniline tõend tunnistatakse pärast algset väljastamist kehtetuks, kaotab see kehtivuse alates kehtetuks tunnistamise hetkest ja selle staatust ei saa mingil juhul ennistada.

5. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused kvalifitseeritud elektrooniliste tõendite jaoks. Nimetatud rakendusaktid peavad olema kooskõlas artikli 5a lõikes 23 osutatud rakendusaktidega, mis käsitlevad Euroopa digiidentiteedikukru rakendamist. Need võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 45e

Atribuutide kontrollimine autentsete allikate alusel

1. Liikmesriigid tagavad 24 kuu jooksul pärast artikli 5a lõikes 23 ja artikli 5c lõikes 6 osutatud rakendusaktide jõustumise kuupäeva, et vähemalt VI lisas loetletud atribuutide puhul, kui need atribuudid põhinevad avaliku sektori autentsetel allikatel, võetakse meetmed, mis võimaldavad elektrooniliste tõendite kvalifitseeritud usaldusteenuse osutajatel neid atribuute kasutaja taotlusel kooskõlas liidu või riigisisese õigusega elektrooniliselt kontrollida.

2. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon, võttes arvesse asjakohaseid rahvusvahelisi standardeid, rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused atribuutide kataloogi jaoks, kavad atribuutide tõendamise jaoks ning käesoleva artikli lõike 1 kohaldamiseks kvalifitseeritud elektrooniliste tõendite kontrolli menetlused. Nimetatud rakendusaktid peavad olema kooskõlas artikli 5a lõikes 23 osutatud rakendusaktidega, mis käsitlevad Euroopa digiidentiteedikukru rakendamist. Need võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 45f

Autentse allika eest vastutava avaliku sektori asutuse või tema nimel välja antud elektroonilistele tõenditele esitatavad nõuded

1. Autentse allika eest vastutava avaliku sektori asutuse või tema nimel välja antud elektrooniline tõend peab vastama järgmistele nõuetele:

   a) VII lisas sätestatud nõuded;

   b) VII lisa punktis b osutatud väljaandjana tuvastatud ja artikli 3 punktis 46 osutatud avaliku sektori asutuse kvalifitseeritud e-allkirja või kvalifitseeritud e-templit toetav kvalifitseeritud sertifikaat sisaldab automaatseks töötlemiseks sobivas formaadis konkreetseid sertifitseeritud atribuute,

      i) millest nähtub, et väljastav asutus on asutatud vastavalt liidu või riigisisesele õigusele asutusena, mis vastutab autentse allika eest, mille alusel elektrooniline tõend välja antakse, või asutusena, mis on määratud tegutsema selle asutuse nimel;

      ii) mis hõlmavad andmeid, mis üheselt mõistetavalt tähistavad alapunktis i osutatud autentset allikat, ning

      iii) milles määratakse kindlaks alapunktis i osutatud liidu või riigisisene õigus.

2. Liikmesriik, kus artikli 3 punktis 46 osutatud avaliku sektori asutused on asutatud, tagab et elektroonilisi tõendeid välja andvad avaliku sektori asutused vastavad samaväärsele usaldusväärsuse tasemele kui kvalifitseeritud usaldusteenuse osutajad vastavalt artiklile 24.

3. Liikmesriigid teavitab artikli 3 punktis 46 osutatud avaliku sektori asutustest komisjoni. See teavitus hõlmab vastavushindamisasutuse koostatud vastavushindamisaruannet, milles kinnitatakse, et käesoleva artikli lõigetes 1, 2 ja 6 sätestatud nõuded on täidetud. Komisjon teeb artikli 3 punktis 46 osutatud avaliku sektori asutuste loetelu turvalise kanali kaudu üldsusele kättesaadavaks automaatseks töötlemiseks sobivas, elektrooniliselt allkirjastatud või e-templiga varustatud formaadis.

4. Kui autentse allika eest vastutava avaliku sektori asutuse poolt või nimel välja antud elektrooniline tõend tunnistatakse pärast algset väljastamist kehtetuks, kaotab see kehtivuse alates kehtetuks tunnistamise hetkest ning selle staatust ei saa ennistada.

5. Kui autentse allika eest vastutava avaliku sektori asutuse poolt või nimel välja antud elektrooniline tõend vastab lõikes 6 osutatud standarditele, kirjeldustele ja menetlustele, loetakse see lõikes 1 sätestatud nõuetele vastavaks.

6. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused autentse allika eest vastutava avaliku sektori asutuse või tema nimel välja antud elektroonilise tõendi jaoks. Nimetatud rakendusaktid peavad olema kooskõlas artikli 5a lõikes 23 osutatud rakendusaktidega, mis käsitlevad Euroopa digiidentiteedikukru rakendamist. Need võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

7. Hiljemalt ... [kuus kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõike 3 kohaldamiseks. Nimetatud rakendusaktid peavad olema kooskõlas artikli 5a lõikes 23 osutatud rakendusaktidega, mis käsitlevad Euroopa digiidentiteedikukru rakendamist. Need võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

8. Artikli 3 punktis 46 osutatud avaliku sektori asutused, kes väljastavad elektroonilisi tõendeid, tagavad liidese artikli 5a kohaselt pakutavate Euroopa digiidentiteedikukrute jaoks.

Artikkel 45g

Elektrooniliste tõendite väljastamine Euroopa digiidentiteedikukrutesse

1. Elektrooniliste tõendite pakkujad annavad Euroopa digiidentiteedikukru kasutajatele võimaluse taotleda, saada, salvestada ja hallata elektroonilist tõendit, olenemata sellest, millises liikmesriigis Euroopa digiidentiteedikukrut pakutakse.

2. Kvalifitseeritud elektrooniliste tõendite pakkujad tagavad liidese artikli 5a kohaselt pakutavate Euroopa digiidentiteedikukrute jaoks.

Artikkel 45h

Täiendavad normid elektroonilise tõendi teenuste osutamiseks

1. Kvalifitseeritud ja kvalifitseerimata elektrooniliste tõendite teenuste osutajad ei tohi kombineerida selliste teenuste osutamisega seotud isikuandmeid enda või oma äripartnerite pakutavate muude teenustega seotud isikuandmetega.

2. Elektrooniliste tõendite teenuste osutamisega seotud isikuandmeid hoitakse elektrooniliste tõendite pakkuja valduses olevatest muudest andmetest loogiliselt eraldi.

3. Kvalifitseeritud elektrooniliste tõendite teenuste osutajad tagavad, et selliseid kvalifitseeritud usaldusteenuseid osutatakse muudest nende osutatavatest teenustest funktsionaalselt eraldi.

10. JAGU

ELEKTROONILISE ARHIVEERIMISE TEENUSED

Artikkel 45i

Elektroonilise arhiveerimise teenuse õiguslik toime

1. Elektrooniliste andmete ja e-dokumentide, mille säilitamiseks kasutatakse elektroonilise arhiveerimise teenust, õigusjõudu ega kohtumenetluses tõendina lubatavust ei tohi välistada üksnes seetõttu, et need on elektroonilisel kujul või et nende säilitamiseks ei kasutata kvalifitseeritud elektroonilise arhiveerimise teenust.

2. Kvalifitseeritud elektroonilise arhiveerimise teenuse abil säilitatavate elektrooniliste andmete ja e-dokumentide puhul kehtib nende kvalifitseeritud usaldusteenuse osutaja poolt säilitamise ajal andmete tervikluse ja päritolu presumptsioon.

Artikkel 45j

Kvalifitseeritud elektroonilise arhiveerimise teenustele esitatavad nõuded

1. Kvalifitseeritud elektroonilise arhiveerimise teenused vastavad järgmistele nõuetele:

   a) neid osutavad kvalifitseeritud usaldusteenuse osutajad;

   b) nende puhul kasutatakse menetlusi ja tehnoloogiat, millega on võimalik tagada elektrooniliste andmete ja e-dokumentide säilivus ja loetavus ka pärast nende tehnoloogilise kehtivusaja lõppemist ja vähemalt kogu nende õigusliku või lepingujärgse säilitamisaja jooksul, säilitades samal ajal nende tervikluse ja nende päritolu täpsuse;

c) nende puhul on tagatud, et elektroonilisi andmeid ja e-dokumente säilitatakse selliselt, et need on kaitstud kaotsimineku ja muutmise eest, välja arvatud muudatused seoses andmekandja või andmete elektroonilise vorminguga;

d) need võimaldavad volitatud tuginevatel isikutel saada automaatselt teate, mis kinnitab, et kvalifitseeritud elektroonilisest arhiivist saadud elektrooniliste andmete ja e-dokumentide puhul kehtib andmetervikluse presumptsioon nende säilitamisaja algusest kuni otsingu hetkeni.

Esimese lõigu punktis d osutatud teade esitatakse usaldusväärsel ja tõhusal viisil ning see ning sellel on kvalifitseeritud elektroonilise arhiveerimise teenuse osutaja kvalifitseeritud e-allkiri või kvalifitseeritud e-tempel.

2. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused kvalifitseeritud elektroonilise arhiveerimise teenuste jaoks. Kui kvalifitseeritud elektroonilise arhiveerimise teenus vastab kõnealustele standarditele, kirjeldustele ja menetlustele, loetakse kvalifitseeritud elektroonilise arhiveerimise teenustele esitatavad nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

11. JAGU

ELEKTRONILISED ARVESTUSRAAMATUD

Artikkel 45k

Elektrooniliste arvestusraamatute õiguslik toime

1. Elektroonilise arvestusraamatu õigusjõudu ega kohtumenetluses tõendina lubatavust ei tohi välistada üksnes seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud elektroonilistele arvestusraamatutele esitatavatele nõuetele.

2. Kvalifitseeritud elektroonilises arvestusraamatus sisalduvate andmekirjete puhul kehtib nende kordumatu ja täpse kronoloogilise järjestuse ning tervikluse presumptsioon.

Artikkel 45l

Kvalifitseeritud elektroonilistele arvestusraamatutele esitatavad nõuded

1. Kvalifitseeritud elektroonilised arvestusraamatud vastavad järgmistele nõuetele:

   a) need on loonud ja neid haldab üks või mitu kvalifitseeritud usaldusteenuse osutajat;

   b) neis määratakse kindlaks arvestusraamatusse kantud andmekirjete päritolu;

   c) need tagavad arvestusraamatusse kantud andmekirjete kordumatu kronoloogilise järjestuse;

   d) neisse kantakse andmeid sellisel viisil, et kõik hilisemad andmete muudatused on kohe tuvastatavad, tagades andmete tervikluse ajas.

2. Kui elektrooniline arvestusraamat vastab lõikes 3 osutatud standarditele, kirjeldustele ja menetlustele, loetakse lõikes 1 sätestatud nõuded täidetuks.

3. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega võrdlusstandardite loetelu ning vajaduse korral kirjeldused ja menetlused käesoleva artikli lõikes 1 sätestatud nõuete jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

47) Lisatakse järgmine peatükk:

„PEATÜKK IVa
JUHTIMISRAAMISTIK

Artikkel 46a
Euroopa digiidentiteedikukru raamistiku järelevalve

1. Liikmesriigid määravad oma territooriumil ühe või mitu järelevalveasutust.

Esimese lõigu kohaselt määratud järelevalveasutustele antakse oma ülesannete tulemuslikuks, tõhusaks ja sõltumatuks täitmiseks vajalikud volitused ja piisavad vahendid.

2. Liikmesriigid teatavad põhjendamatu viivituseta komisjonile lõike 1 kohaselt määratud järelevalveasutuste nimed ja aadressid ning nende hilisemad muudatused. Komisjon avaldab teatatud järelevalveasutuste loetelu.

3. Lõike 1 kohaselt määratud järelevalveasutuste roll on

   a) teha järelevalvet määrava liikmesriigi territooriumil asutatud Euroopa digiidentiteedikukrute pakkujate üle ning tagada eelneva ja järgneva järelevalve käigus, et need pakkujad ja nende pakutavad Euroopa digiidentiteedikukrud vastaksid käesolevas määruses sätestatud nõuetele;

   b) võtta vajaduse korral järgneva järelevalve käigus meetmeid määrava liikmesriigi territooriumil asutatud Euroopa digiidentiteedikukrute pakkujate suhtes, kui nad on saanud teavet, et pakkujad või nende pakutavad Euroopa digiidentiteedikukrud rikuvad käesolevat määrust.

4. Lõike 1 kohaselt määratud järelevalveasutustel on eelkõige järgmised ülesanded:

   a) teha koostööd teiste järelevalveasutustega ja anda neile abi kooskõlas artiklitega 46c ja 46e;

   b) nõuda teavet, mida on vaja käesoleva määruse täitmise üle seire tegemiseks;

c) teavitada direktiivi (EL) 2022/2555 artikli 8 lõike 1 alusel määratud või asutatud asjaomaseid pädevaid asutusi igast olulisest turvarikkumisest või tervikluse kaost, millest nad oma ülesannete täitmisel teada saavad, ning teavitada teisi liikmesriike puudutava olulise turvarikkumise või tervikluse kao korral asjaomase liikmesriigi direktiivi (EL) 2022/2555 artikli 8 lõike 3 alusel määratud või asutatud ühtset kontaktpunkti ja teistes asjaomastes liikmesriikides käesoleva määruse artikli 46c lõike 1 alusel määratud ühtseid kontaktpunkte, samuti teavitada üldsust või nõuda, et Euroopa digiidentiteedikukru pakkujad seda teeks, kui nad on teinud kindlaks, et turvarikkumise või tervikluse kao avalikustamine oleks üldsuse huvides;

d) teha kohapealseid kontrolle ja kaugjärelevalvet;

e) nõuda Euroopa digiidentiteedikukrute pakkujatelt käesolevas määruses sätestatud nõuete täitmata jätmise heastamist;

f) peatada või tühistada tuginevate isikute registreerimine ja kaasamine artikli 5b lõikes 7 osutatud mehhanismi Euroopa digiidentiteedikukru ebaseadusliku või petturliku kasutamise korral;

g) teha koostööd määruse (EL) 2016/679 artikli 51 kohaselt asutatud pädevate järelevalveasutustega, eelkõige teavitades neid põhjendamatu viivituseta sellest, kui isikuandmete kaitse reegleid näib olevat rikutud, ja turvarikkumistest, mis näivad kujutavat endast isikuandmetega seotud rikkumisi.

5. Kui lõike 1 kohaselt määratud järelevalveasutus nõuab Euroopa digiidentiteedikukru pakkujalt käesoleva määruse kohaste nõuete täitmata jätmise heastamist vastavalt lõike 4 punktile e ning kõnealune pakkuja ei tegutse vastavalt, ja kui see on kohaldatav, kõnealuse järelevalveasutuse kehtestatud tähtaja jooksul, võib lõike 1 kohaselt määratud järelevalveasutus, võttes eelkõige arvesse sellise rikkumise ulatust, kestust ja tagajärgi, anda pakkujale korralduse peatada või lõpetada Euroopa digiidentiteedikukru pakkumine. Järelevalveasutus teavitab põhjendamatu viivituseta teiste liikmesriikide järelevalveasutusi, komisjoni, tuginevaid isikuid ja Euroopa digiidentiteedikukru kasutajaid otsusest nõuda Euroopa digiidentiteedikukru pakkumise peatamist või lõpetamist.

6. Iga lõike 1 kohaselt määratud järelevalveasutus esitab komisjonile iga aasta 31. märtsiks aruande oma eelneva kalendriaasta põhitegevuse kohta. Komisjon teeb kõnealused aastaaruanded Euroopa Parlamendile ja nõukogule kättesaadavaks.

7. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega käesoleva artikli lõikes 6 osutatud aruandluse formaadid ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 46b

Usaldusteenuste järelevalve

1. Liikmesriigid määravad oma territooriumil asutatud järelevalveasutuse või vastastikusel kokkuleppel teise liikmesriigiga määravad kõnealuses teises liikmesriigis asutatud järelevalveasutuse. Nimetatud järelevalveasutus vastutab määravas liikmesriigis usaldusteenustega seotud järelevalveülesannete täitmise eest.

   Esimese lõigu kohaselt määratud järelevalveasutustele antakse oma ülesannete täitmiseks vajalikud volitused ja piisavad vahendid.

2. Liikmesriigid teatavad põhjendamatu viivituseta komisjonile oma lõike 1 kohaselt määratud järelevalveasutuste nimed ja aadressid ning nende hilisemad muudatused. Komisjon avaldab teatatud järelevalveasutuste loetelu.

3. Lõike 1 kohaselt määratud järelevalveasutuste roll on

   a) teha järelevalvet määrava liikmesriigi territooriumil asutatud kvalifitseeritud usaldusteenuse osutajate üle ning tagada eelneva ja järgneva järelevalve käigus, et kvalifitseeritud usaldusteenuse osutajad ja nende osutatavad kvalifitseeritud usaldusteenused vastaksid käesolevas määruses sätestatud nõuetele;

   b) võtta järgneva järelevalve käigus vajaduse korral meetmeid määrava liikmesriigi territooriumil asutatud kvalifitseerimata usaldusteenuse osutajate suhtes, kui järelevalveasutusele teatatakse, et kvalifitseerimata usaldusteenuse osutajad või nende osutatavad usaldusteenused ei vasta väidetavalt käesolevas määruses sätestatud nõuetele.

4. Lõike 1 kohaselt määratud järelevalveasutusel on eelkõige järgmised ülesanded:

a) teavitada direktiivi (EL) 2022/2555 artikli 8 lõike 1 alusel määratud või asutatud asjaomaseid pädevaid asutusi igast olulisest turvarikkumisest või tervikluse kaost, millest ta oma ülesannete täitmisel teada saab, ning teavitada teisi liikmesriike puudutava olulise turvarikkumise või tervikluse kao korral asjaomase liikmesriigi direktiivi (EL) 2022/2555 artikli 8 lõike 3 alusel määratud või asutatud ühtset kontaktpunkti ja teistes asjaomastes liikmesriikides käesoleva määruse artikli 46c lõike 1 alusel määratud ühtseid kontaktpunkte, samuti teavitada üldsust või nõuda, et usaldusteenuse osutaja seda teeks, kui järelevalveasutus on teinud kindlaks, et turvarikkumise või tervikluse kao avalikustamine oleks üldsuse huvides;

b) teha koostööd teiste järelevalveasutustega ja anda neile abi kooskõlas artiklitega 46c ja 46e;

c) analüüsida artikli 20 lõikes 1 ja artikli 21 lõikes 1 osutatud vastavushindamisaruandeid;

d) anda komisjonile aru oma põhitegevusest kooskõlas käesoleva artikli lõikega 6;

e) korraldada auditeid või paluda vastavushindamisasutusel teha kvalifitseeritud usaldusteenuse osutajate vastavushindamine kooskõlas artikli 20 lõikega 2;

f) teha koostööd määruse (EL) 2016/679 artikli 51 kohaselt asutatud pädevate järelevalveasutustega, eelkõige teavitades neid põhjendamatu viivituseta sellest, kui isikuandmete kaitse reegleid näib olevat rikutud, ja turvarikkumistest, mis näivad kujutavat endast isikuandmetega seotud rikkumisi.

g) anda usaldusteenuse osutajatele ja nende osutatavatele teenustele kvalifitseeritud staatus ning võtta see staatus ära kooskõlas artiklitega 20 ja 21;

h) teavitada artikli 22 lõikes 3 osutatud riigisiseste usaldusnimekirjade eest vastutavat asutust oma otsustest anda kvalifitseeritud staatus või võtta see ära, välja arvatud juhul, kui kõnealune asutus on samuti lõike 1 kohaselt määratud järelevalveasutus;

i) kontrollida lõpetamiskava käsitlevate sätete olemasolu ja nõuetekohast kohaldamist, kui kvalifitseeritud usaldusteenuse osutaja lõpetab oma tegevuse, sealhulgas seda, kuidas teave hoitakse kättesaadavana kooskõlas artikli 24 lõike 2 punktiga h;

j) nõuda usaldusteenuse osutajatelt käesolevas määruses sätestatud nõuete täitmata jätmise heastamist;

k) uurida veebibrauserite pakkujate poolt artikli 45a kohaselt esitatud väiteid ja võtta vajaduse korral meetmeid.

5. Liikmesriigid võivad nõuda, et lõike 1 kohaselt määratud järelevalveasutus looks, haldaks ja ajakohastaks usaldusteenuste taristut kooskõlas riigisisese õigusega.

6. Iga lõike 1 kohaselt määratud järelevalveasutus esitab komisjonile iga aasta 31. märtsiks aruande oma eelneva kalendriaasta põhitegevuse kohta. Komisjon teeb kõnealused aastaaruanded Euroopa Parlamendile ja nõukogule kättesaadavaks.

7. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] võtab komisjon vastu suunised, mis käsitlevad käesoleva artikli lõikes 4 osutatud ülesannete täitmist lõike 1 kohaselt määratud järelevalveasutuste poolt, ning kehtestab rakendusaktidega käesoleva artikli lõikes 6 osutatud aruandluse formaadid ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 46c
Ühtsed kontaktpunktid

1. Iga liikmesriik määrab usaldusteenuste, Euroopa digiidentiteedikukrute ja teavitatud e-identimise süsteemide jaoks ühtse kontaktpunkti.

2. Iga ühtne kontaktpunkt täidab sidepidamisfunktsiooni, et hõlbustada piiriülest koostööd usaldusteenuse osutajate järelevalveasutuste vahel ja Euroopa digiidentiteedikukrute pakkujate järelevalveasutuste vahel ning asjakohastel juhtudel komisjoni ja Euroopa Liidu Küberturvalisuse Ametiga (ENISA) ja muude oma liikmesriigi pädevate asutustega.

3. Iga liikmesriik avalikustab ja teatab põhjendamatu viivituseta komisjonile lõike 1 kohaselt määratud ühtse kontaktpunkti nimed ja aadressid ning nende hilisemad muudatused.

4. Komisjon avaldab lõike 3 kohaselt teatatud ühtsete kontaktpunktide loetelu.

Artikkel 46d

Vastastikune abi

1. Selleks et hõlbustada käesolevast määrusest tulenevate kohustuste üle tehtavat järelevalvet ja täitmise tagamist, võivad artikli 46a lõike 1 ja artikli 46b lõike 1 kohaselt määratud järelevalveasutused taotleda, sealhulgas artikli 46e lõike 1 kohaselt loodud koostöörühma kaudu, vastastikust abi sellises teises liikmesriigis asuvatelt järelevalveasutustelt, kus Euroopa digiidentiteedikukru pakkuja või usaldusteenuse osutaja on asutatud või kus asuvad tema võrgu- ja infosüsteemid või osutatakse tema teenuseid.

2. Vastastikune abi hõlmab vähemalt järgmist:

a) ühes liikmesriigis järelevalve- ja täitemeetmeid kohaldav järelevalveasutus teavitab teise asjaomase liikmesriigi järelevalveasutust ja konsulteerib temaga;

b) järelevalveasutus võib taotleda teise liikmesriigi järelevalveasutuselt järelevalve- või täitemeetmete võtmist, sealhulgas näiteks taotlused artiklites 20 ja 21 osutatud vastavushindamisaruannetega seotud kontrollide tegemiseks seoses usaldusteenuste osutamisega;

c) kui see on asjakohane, võivad järelevalveasutused viia läbi ühiseid uurimisi teiste liikmesriikide järelevalveasutustega.

Asjaomased liikmesriigid lepivad esimese lõigus osutatud ühiste toimingute korras ja protseduurides kokku ning kehtestavad need oma riigisisese õiguse kohaselt.

3. Abitaotluse saanud järelevalveasutus võib taotluse täitmisest keelduda mis tahes järgmisel alusel:

a) taotletav abi ei ole proportsionaalne järelevalveasutuse järelevalvetegevusega vastavalt artiklitele 46a ja 46b;

b) järelevalveasutus ei ole pädev taotletavat abi andma;

c) taotletava abi andmine oleks vastuolus käesoleva määrusega.

4. Artikli 46e lõike 1 kohaselt loodud koostöörühm annab hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] ja seejärel iga kahe aasta tagant välja suunised käesoleva artikli lõigetes 1 ja 2 osutatud vastastikuse abi korralduslike aspektide ja menetluse kohta.

Artikkel 46e

Euroopa digiidentiteedi koostöörühm

1. Selleks et toetada ja hõlbustada liikmesriikide piiriülest koostööd ja teabevahetust usaldusteenuste, Euroopa digiidentiteedikukrute ja teavitatud e-identimise süsteemide kohta, loob komisjon Euroopa digiidentiteedi koostöörühma (edaspidi „koostöörühm“).

2. Koostöörühm koosneb liikmesriikide ja komisjoni määratud esindajatest. Koostöörühma juhib komisjon. Komisjon tagab koostöörühmale sekretariaadi.

3. Asjaomaste sidusrühmade esindajaid võib vastavalt vajadusele kutsuda osalema vaatlejatena koostöörühma koosolekutel ja selle töös.

4. ENISA kutsutakse osalema vaatlejana koostöörühma töös, kui koostöörühm vahetab arvamusi, parimaid tavasid ja teavet asjakohaste küberturvalisuse aspektide kohta, nagu turvarikkumistest teatamine, ning kui käsitletakse küberturvalisuse sertifikaatide või standardite kasutamist.

5. Koostöörühmal on järgmised ülesanded:

   a) pidada komisjoniga nõu ja teha temaga koostööd uute poliitiliste algatuste osas digiidentiteedikukrute, e-identimise vahendite ja usaldusteenuste valdkonnas;

   b) nõustada kohasel viisil komisjoni käesoleva määruse kohaselt vastuvõetavate rakendusaktide ja delegeeritud õigusaktide eelnõude ettevalmistamise varajases etapis;

   c) selleks et toetada järelevalveasutusi käesoleva määruse sätete rakendamisel,

      i) vahetada parimaid tavasid ja teavet käesoleva määruse sätete rakendamise kohta;

      ii) hinnata asjakohaseid arengusuundi digiidentiteedikukrute, e-identimise ja usaldusteenuste sektoris;

      iii) korraldada ühiskoosolekuid asjaomaste huvitatud pooltega kogu liidust, et arutada koostöörühma tegevust ja koguda teavet esilekerkivate poliitikaprobleemide kohta;

iv) vahetada ENISA toetusel arvamusi, parimaid tavasid ja teavet Euroopa digiidentiteedikukrute, e-identimise süsteemide ja usaldusteenuste asjakohaste küberturvalisuse aspektide kohta;

v) vahetada parimaid tavasid seoses artiklites 5e ja 10 osutatud turvarikkumistest teatamise ja ühismeetmete alase poliitika väljatöötamise ja rakendamisega;

vi) korraldada ühiskoosolekuid direktiivi (EL) 2022/2555 artikli 14 lõike 1 kohaselt loodud võrgu- ja infoturbe koostöörühmaga, et vahetada asjakohast teavet usaldusteenuste ja e-identimisega seotud küberohtude, intsidentide, nõrkuste, teadlikkuse suurendamise algatuste, koolituste, õppuste ja oskuste, suutlikkuse suurendamise, standardite ja tehniliste kirjelduste alase suutlikkuse ning standardite ja tehniliste kirjelduste kohta;

vii) arutada järelevalveasutuse taotlusel konkreetseid vastastikuse abi taotlusi, nagu on osutatud artiklis 46d;

viii) hõlbustada teabevahetust järelevalveasutuste vahel, andes suuniseid artiklis 46d osutatud vastastikuse abi korralduslike aspektide ja menetluste kohta;

d) korraldada selliste e-identimise süsteemide vastastikuseid hindamisi, millest tuleb käesoleva määruse kohaselt teavitada.

6. Liikmesriigid tagavad koostöörühmas enda määratud esindajate tulemusliku ja tõhusa koostöö.

7. Hiljemalt ... [12 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] kehtestab komisjon rakendusaktidega vajaliku korra käesoleva artikli lõike 5 punktis d osutatud liikmesriikidevahelise koostöö hõlbustamiseks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

48) Artiklit 47 muudetakse järgmiselt:

a) lõiked 2 ja 3 asendatakse järgmisega:

„2. Artikli 5c lõikes 7, artikli 24 lõikes 4b ja artikli 30 lõikes 4 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile määramata ajaks alates 17. septembrist 2014.

3. Euroopa Parlament või nõukogu võib artikli 5c lõikes 7, artikli 24 lõikes 4b ja artikli 30 lõikes 4 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.“;

b) lõige 5 asendatakse järgmisega:

„5. Artikli 5c lõike 7, artikli 24 lõike 4b või artikli 30 lõike 4 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle suhtes vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.“

49) VI peatükki lisatakse järgmised artiklid:

„*Artikkel 48a*
Aruandlusnõuded

1. Liikmesriigid tagavad nende territooriumil pakutavate Euroopa digiidentiteedikukrute ja kvalifitseeritud usaldusteenuste toimimist käsitleva statistika kogumise.

2. Lõike 1 kohaselt kogutud statistika hõlmab järgmist:

a) nende füüsiliste ja juriidiliste isikute arv, kellel on kehtiv Euroopa digiidentiteedikukkur;

b) nende teenuste liik ja arv, mille puhul aktsepteeritakse Euroopa digiidentiteedikukru kasutamist;

c) tuginevate isikute ja kvalifitseeritud usaldusteenustega seotud kasutajapoolsete kaebuste ja tarbijakaitse- või andmekaitsealaste intsidentide arv;

d) koondaruanne, mis sisaldab andmeid Euroopa digiidentiteedikukru kasutamist takistavate intsidentide kohta;

e) kokkuvõttev teave Euroopa digiidentiteedikukrute või kvalifitseeritud usaldusteenuste oluliste turvaintsidentide, andmetega seotud rikkumiste ja mõjutatud kasutajate kohta.

3. Lõikes 2 osutatud statistika tehakse üldsusele kättesaadavaks avatud ja üldkasutatavas masinloetavas vormingus.

4. Liikmesriigid esitavad komisjonile iga aasta 31. märtsiks aruande lõike 2 kohaselt kogutud statistika kohta.“

50) Artikkel 49 asendatakse järgmisega:

„*Artikkel 49*
Läbivaatamine

1. Komisjon vaatab läbi käesoleva määruse kohaldamise ning esitab Euroopa Parlamendile ja nõukogule selle kohta hiljemalt ... [24 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva] aruande. Nimetatud aruandes hindab komisjon eelkõige seda, kas on asjakohane muuta käesoleva määruse kohaldamisala või selle teatavaid sätteid, sealhulgas eelkõige artikli 5c lõike 5 sätteid, võttes arvesse käesoleva määruse kohaldamisel saadud kogemusi ning tehnoloogia, turu ja õiguse arengut. Vajaduse korral lisatakse aruandele käesoleva määruse muutmise ettepanek.

2. Lõikes 1 osutatud aruanne sisaldab hinnangut käesoleva määruse kohaldamisalasse kuuluvate teavitatud e-identimise vahendite ja Euroopa digiidentiteedikukrute kättesaadavuse, turvalisuse ja kasutatavuse kohta ning hinnangut selle kohta, kas kõigil eraõiguslikel internetipõhise teenuse osutajatel, kes tuginevad kasutajate autentimisel kolmanda isiku e-identimise teenustele, on kohustus aktsepteerida teavitatud e-identimise vahendite ja Euroopa digiidentiteedikukru kasutamist.

3. Komisjon esitab hiljemalt … [6 aastat pärast käesoleva muutmismääruse jõustumise kuupäeva] ja seejärel iga nelja aasta tagant Euroopa Parlamendile ja nõukogule aruande edusammudest käesoleva määruse eesmärkide saavutamisel.“

51) Artikkel 51 asendatakse järgmisega:

„*Artikkel 51*
Üleminekumeetmed

1. Turvalisi allkirja andmise vahendeid, mille vastavus on kindlaks määratud vastavalt direktiivi 1999/93/EÜ artikli 3 lõikele 4, käsitatakse käesoleva määruse kohaselt jätkuvalt kvalifitseeritud e-allkirja andmise vahenditena kuni ... [36 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva].

2. Direktiivi 1999/93/EÜ kohaselt füüsilistele isikutele väljastatud kvalifitseeritud sertifikaate käsitatakse käesoleva määruse kohaselt jätkuvalt e-allkirjade kvalifitseeritud sertifikaatidena kuni ... [24 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva].

3. Kvalifitseeritud e-allkirja ja kvalifitseeritud e-templi kaugloomise vahendeid võivad hallata muud kvalifitseeritud usaldusteenuse osutajad, kui need kvalifitseeritud usaldusteenuse osutajad, kes osutavad kvalifitseeritud usaldusteenuseid kvalifitseeritud e-allkirjade ja kvalifitseeritud e-templite kaugloomise vahendite haldamiseks kooskõlas artiklitega 29a ja 39a, ilma et nende haldamisteenuste osutamiseks oleks vaja kvalifitseeritud staatust, kuni ... [24 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva].

4. Kvalifitseeritud usaldusteenuse osutajad, kellele on käesoleva määruse alusel antud kvalifitseeritud staatus enne ... [käesoleva muutmismääruse jõustumise kuupäev], esitavad järelevalveasutusele artikli 24 lõigete 1a ja 1b nõuetele vastavust tõendava vastavushindamisaruande niipea kui võimalik ja igal juhul hiljemalt ... [24 kuud pärast käesoleva muutmismääruse jõustumise kuupäeva].“

52) I–IV lisa muudetakse vastavalt käesoleva määruse I–IV lisale.

53) Uute lisadena lisatakse käesoleva määruse V, VI ja VII lisas esitatud V, VI ja VII lisa.

Artikkel 2

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

I LISA

Määruse (EL) nr 910/2014 I lisa punkt i asendatakse järgmisega:

„i) teave kvalifitseeritud sertifikaadi kehtivuse kohta või selle kohta, kus asuvad teenused, mida saab kasutada kvalifitseeritud sertifikaadi kehtivuse kohta teabe saamiseks;“.

II LISA

Määruse (EL) nr 910/2014 II lisa punktid 3 ja 4 jäetakse välja.

III LISA

Määruse (EL) nr 910/2014 III lisa punkt i asendatakse järgmisega:

„i) teave kvalifitseeritud sertifikaadi kehtivuse kohta või selle kohta, kus asuvad teenused, mida saab kasutada kvalifitseeritud sertifikaadi kehtivuse kohta teabe saamiseks;“.

IV LISA

Määruse (EL) nr 910/2014 IV lisa muudetakse järgmiselt.

1) Punkt c asendatakse järgmisega:

„c) kui tegemist on füüsilise isikuga: vähemalt selle isiku nimi või varjunimi, kellele sertifikaat on väljastatud; kui kasutatakse varjunime, on varjunime kasutus selgesti näidatud;

ca) kui tegemist on juriidilise isikuga: seda juriidilist isikut, kellele sertifikaat on väljastatud, üheselt mõistetavalt tähistavad andmed, mis sisaldavad vähemalt selle juriidilise isiku nime, kellele sertifikaat on väljastatud, ja olemasolu korral registrinumbrit, nagu see on esitatud ametlikes dokumentides;“

2) punkt j asendatakse järgmisega:

„j) teave kvalifitseeritud sertifikaadi kehtivuse kohta või selle kohta, kus asuvad teenused, mida saab kasutada kvalifitseeritud sertifikaadi kehtivuse kohta teabe saamiseks.“

V LISA

„V LISA

KVALIFITSEERITUD ELEKTROONILISTELE TÕENDITELE ESITATAVAD NÕUDED

Kvalifitseeritud elektroonilised tõendid sisaldavad järgmist:

a) vähemalt automaatseks töötlemiseks sobivas formaadis märge selle kohta, et tõend on väljastatud kvalifitseeritud elektroonilise tõendina;

b) andmed, mis üheselt mõistetavalt tähistavad kvalifitseeritud elektroonilisi tõendeid väljastavat kvalifitseeritud usaldusteenuse osutajat, sealhulgas vähemalt selle liikmesriigi nimi, kus on teenuseosutaja asukoht, ning

   i) juriidilise isiku puhul nimi ja olemasolu korral registrinumber, nagu see on esitatud ametlikes dokumentides,

   ii) füüsilise isiku puhul isiku nimi;

c) andmed, mis üheselt mõistetavalt tähistavad üksust, kellele tõendatud atribuudid viitavad; kui kasutatakse varjunime, on varjunime kasutus selgesti näidatud;

d) tõendatud atribuut või atribuudid, sealhulgas olemasolu korral teave, mida on vaja, et teha kindlaks nende atribuutide kohaldamisala;

e) üksikasjalikud andmed tõendi kehtivusaja alguse ja lõpu kohta;

f) tõendi identifitseerimiskood, mis peab olema iga kvalifitseeritud usaldusteenuse osutaja puhul kordumatu, ja olemasolu korral märge tõendite süsteemi kohta, kuhu tõend kuulub;

g) väljastava kvalifitseeritud usaldusteenuse osutaja kvalifitseeritud e-allkiri või kvalifitseeritud e-tempel;

h) koht, kus punktis g osutatud kvalifitseeritud e-allkirja või kvalifitseeritud e-templit toetav sertifikaat on tasuta kättesaadav;

i) teave kvalifitseeritud tõendi kehtivuse kohta või selle kohta, kus asuvad teenused, mida saab kasutada kvalifitseeritud tõendi kehtivuse kohta teabe saamiseks.“

VI LISA

„VI LISA

ATRIBUUTIDE MIINIMUMLOETELU

Vastavalt artiklile 45e tagavad liikmesriigid, et võetakse meetmeid, et võimaldada elektrooniliste tõendite kvalifitseeritud usaldusteenuse osutajatel kontrollida kasutaja taotlusel elektrooniliste vahendite abil järgmiste atribuutide autentsust asjaomasest autentsest allikast riiklikul tasandil või määratud vahendajate kaudu, kes on liidu või riigisisese õiguse kohaselt riiklikul tasandil tunnustatud ja juhul, kui need atribuudid põhinevad avaliku sektori autentsetel allikatel:

1. aadress;

2. vanus;

3. sugu;

4. perekonnaseis;

5. perekonna koosseis;

6. rahvus või kodakondsus;

7. haridusalane kvalifikatsioon, kraadid ja diplomid;

8. kutsekvalifikatsioon, kutsenimetused ja litsentsid;

9. füüsiliste või juriidiliste isikute esindamise volitused;

10. avalikud load ja litsentsid;

11. kui tegemist on juriidilise isikuga: finants- ja äriühinguandmed.“

VII LISA

„VII LISA

AUTENTSE ALLIKA EEST VASTUTAVA AVALIKU SEKTORI ASUTUSE VÕI TEMA NIMEL VÄLJA ANTUD ELEKTROONILISTELE TÕENDITELE ESITATAVAD NÕUDED

Autentse allika eest vastutava avaliku sektori asutuse või tema nimel välja antud elektrooniline tõend hõlmab järgmist:

a) vähemalt automaatseks töötlemiseks sobivas formaadis märge selle kohta, et tõend on väljastatud autentse allika eest vastutava avaliku sektori asutuse või tema nimel välja antud elektroonilise tõendina;

b) andmed, mis üheselt mõistetavalt tähistavad elektroonilisi tõendeid väljastavat avaliku sektori asutust ning sisaldavad vähemalt selle liikmesriigi nime, kõnealuse avaliku sektori asutuse asukohta, asutuse nime ja olemasolu korral registrinumbrit, nagu see on esitatud ametlikes dokumentides;

c) andmed, mis üheselt mõistetavalt tähistavad üksust, kellele tõendatud atribuudid viitavad; kui kasutatakse varjunime, on varjunime kasutus selgesti näidatud;

d) tõendatud atribuut või atribuudid, sealhulgas olemasolu korral teave, mida on vaja, et teha kindlaks nende atribuutide kohaldamisala;

e) üksikasjalikud andmed tõendi kehtivusaja alguse ja lõpu kohta;

f) tõendi identifitseerimiskood, mis peab olema iga väljastava avaliku sektori asutuse puhul kordumatu, ja olemasolu korral märge tõendite süsteemi kohta, kuhu tõend kuulub;

g) väljastava asutuse kvalifitseeritud e-allkiri või kvalifitseeritud e-tempel;

h) koht, kus punktis g osutatud kvalifitseeritud e-allkirja või kvalifitseeritud e-templit toetav sertifikaat on tasuta kättesaadav;

i) teave tõendi kehtivuse kohta või selle kohta, kus asuvad teenused, mida saab kasutada tõendi kehtivuse kohta teabe saamiseks.“